(6) 80

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-176419

(43)Date of publication of application : 21.06.2002

---

(51)Int.Cl. H04L 9/08
H04N 5/91
H04N 5/92
H04N 7/08
H04N 7/081
H04N 7/167

---

(21)Application number : 2000-370936 (71)Applicant : HITACHI LTD

(22)Date of filing : 06.12.2000 (72)Inventor : YAMAZAKI IORI
HARADA HIROMI
KONISHI KAORU

---

(54) RIGHT PROTECTION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To protect a copyright of contents stored in a storage medium and each right of broadcast enterprises and users.
SOLUTION: In order to protect the copyright of contents that is stored in a storage medium and carried and the right of broadcast enterprises and users, a transmitter side encrypts the contents, set its key to meta data, encrypts the meta data by using a different key, and distributes the encrypted contents and the encrypted meta data as a set. A reception terminal decodes first the encrypted meta data in the encrypted

contents and the encrypted meta data received by the terminal, acquires the key for the contents, and stores the key to a key table in the reception terminal where the security is secured. Then, the reception terminal again encrypts the meta data by using the key the same as that of the contents and stores the encrypted contents and the encrypted meta data to an HDD. When viewed contents are selected, the terminal reads the meta data from the HDD, acquires the key from the key table and decodes the meta data. After a view contract, the keys for the contents and the meta data are stored in a personal mobile CA(Conditional Access) module. Then, by using the contents key, the encrypted contents are decodes to allow user to view the contents.

CLAIMS

[Claim(s)]
[Claim 1]A right protection method comprising:
A limited reception step which generates an event which decrypts a received scramble key (Ks) using the 2nd personal key (km1) memorized by the 1st module in a receiver, and contains enciphered content and encryption metadata using a scramble key (Ks).
Including contents and a copyright protection code step for right protection of metadata, said copyright protection code step, A step which decrypts the 1st received encryption work key (Kw2') using the 1st personal key (km2) recorded on the 2nd module or lock management center, and generates the 1st work key (Kw2).
A step which asks for the 1st contents key (Kk) that decrypted encryption metadata and was contained there using the 1st decrypted work key (Kw2).
A step which enciphers metadata with a contents key (Kk), and a step which accumulates encryption metadata and enciphered content in a recording medium, A step which reads code metadata in a recording medium and is double-sign-ized with a contents key (Kk), a step which accumulates a part of metadata in the 2nd module,

and a step which decrypts enciphered content using the 1st called-for contents key (Kk), and generates contents.

[Claim 2]Viewing-and-listening contract processing which judges whether information on the 2nd module fulfills a viewing condition when viewing and listening is chosen, A right protection method according to claim 1 which includes further metadata processing which accumulates metadata in a recording medium, and contents decoding processing which reads contracted contents from a recording medium using an individual profile's information.

[Claim 3]Viewing-and-listening contract processing which judges whether information on the 2nd module fulfills a storage condition when accumulating is chosen, Metadata processing which accumulates metadata in a removable media, and removable media accumulation processing which accumulates enciphered content in a removable media, A right protection method according to claim 1 or 2 which includes further contents decoding processing which writes information on the 2nd module in a guest profile, and reads contracted contents from removable contents using information on a guest profile.

[Claim 4]Including metadata processing and contents decoding processing further in metadata processing. Divide metadata into the 1st and 2nd metadata, encipher the 1st metadata with a personal key (km2), and it accumulates in the 2nd module, Encipher the 2nd metadata with a disposable key (Kt'), accumulate in a recording medium, read contracted contents from a recording medium using an individual profile's information, and in contents decoding processing. A right protection method according to any one of claims 1 to 3 performing decoding processing of contents according to the 1st and 2nd metadata.

[Claim 5]Including metadata processing and contents decoding processing further in metadata processing. Encipher metadata with a personal key (km2), accumulate in the 2nd module and in contents decoding processing. Write information on the 2nd module in a guest profile, and contracted contents are read from removable contents using information on a guest profile, A right protection method according to any one of claims 1 to 3 performing decoding processing of contents according to metadata and contents.

[Claim 6]A right protection method according to any one of claims 1 to 5 managing a key of a code of contents in said copyright protection code step, and metadata in the lock management center.

[Claim 7]A right protection method according to any one of claims 1 to 6 only information to be protected enciphering metadata and not enciphering information without the necessity for protection in said copyright protection code step.

[Claim 8]In order to set inside of a receiving terminal as personal environment at the time of use, personal environment information area is set up, A right protection

method according to any one of claims 1 to 7, wherein each user acquires information required for generation of personal environment information area from the 2nd module of personal portability and generates personal environment information area at the time of receiving terminal use.

[Claim 9]A right protection method according to any one of claims 1 to 8, wherein information, and a contents key (Kk) and viewing-and-listening contract information of personal environment information area required for generation are stored in the 2nd [of personal portability] module.

[Claim 10]Accumulation by user palatability which made said step to accumulate sources of information of a taste information input by a user, or viewing history information, Request-to-print-out-files accumulation by an electronic program guide which made program arrangement information and program information from metadata sources of information, Or a right protection method according to any one of claims 1 to 9 including either or two or more accumulation processings of compulsive accumulation which a service provider accumulates in a mass storage medium compulsorily within an emergency, a specified time zone, or defined capacity.

[Claim 11]At the time of a gift contract for presenting contents contracted [viewing-and-listening] to the 3rd person, in a removable media Contents contracted [viewing-and-listening] and key information, Or a right protection method according to any one of claims 1 to 10, wherein viewing and listening becomes possible by storing metadata enciphered using a common key or a public key only using a removable media.

[Claim 12]By setting up area which summarized a group member's information at the time of a group contract for setting up a viewing-and-listening contract unit and an accounting unit per group, and storing there viewing-and-listening contract information, A right protection method according to any one of claims 1 to 11 enabling viewing and listening of contents contracted [viewing-and-listening] by a group member.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the right protection method of preventing the illegal use of data in the system which accumulates the digital data distributed especially via a land-based line and satellite connection in the digital state, and uses it, about the right protection method in data distribution service.

[0002]

[Description of the Prior Art]In the conventional digital broadcasting, the contract form which performs a contract that viewing and listening is possible / improper for every service channel, or the contract form which performs the program contract for every time within the same channel existed. In the existing digital broadcasting, in order to make the contents in each contents unit purchase, a user chooses, makes a contract of or determines contents needed, and is made to perform communication by the side of a center after service selection simultaneously with the contract or determination. Purchase of contents of a user is attained by checking the purchase of each contents and transmitting purchase permission data to an after-check contractor by the real time communication a user and by the side of a center. A sale in a contents unit will be made by such a bidirectional real-time purchase method.

[0003]In the digital broadcasting which will start about encryption from now on, the /Carrying-out judgment which enciphers an encryption key usable within a network in a transmission line since the number is being fixed is made. In the present transmission system, after the contents enciphered by the center side perform code release soon after reception within a receiving terminal, they are recorded on a storage device etc. Thus, encryption of the contents at the time of transmission is performed by only the present primary code.

[0004]

[Problem(s) to be Solved by the Invention]However, in the conventional digital broadcasting, although all the servicing information within contract time is acquirable, viewing and listening of only servicing information or the acquisition of only contents which the user chose is difficult.

[0005]In service by digital broadcasting, such as conventional CS/BS, contract offer that it can be viewed and program listened to a contract form in channel viewing-and-listening good / improper one, or the same channel / improper is main. This is because the number of the keys used for the encryption in digital broadcasting has restriction. However, if two or more keys are used, it must become regular transmission of information required in order to solve a code by enciphering the contents in two or more keys, and management of a key must not only become complicated, but must transmit much more information from the present transmission quantity. In few transmitting areas, this is not closely realistic difficult. The thing which increase every day and to lock for every contents is that the number of keys becomes near infinitely, and is dramatically difficult also for this. [of management] Since information required for real-time decoding is always transmitted, the receiving terminal needs to make modules (CA (Conditional Access, limited reception) module), such as a required IC card, always attached to decryption at the time of reception. It is near to encipher contents from these things using two or more keys in the same time of the same program in the same channel difficult.

[0006]In the conventional receiving terminal, it cannot encipher within a receiving

terminal again after code release. Once decrypting the accumulation contents which exist in a receiving terminal etc. from this, it is impossible to make it accumulate by making it encipher again, and the key treatment of the encryption at the time of accumulation, etc. becoming difficult if it accumulates with encryption of a transmission line, and making it encipher and making it accumulate has many various technical problems, such as reliability. Since the information treating the contract of viewing-and-listening good / failure can carry out the whole receiving terminal when receiving digital broadcasting, when the user using a receiving terminal is plurality, the technical problem of being unable to recognize the contract form for every multiple user by the center side occurs.

[0007]Although the form of password embedding, such as digital watermarking, exists as a method of copyright protection demanded, for example in the transfer case to the 3rd person of contents, etc., it is effective to no data formats, and is only protection of only contents. The method which protects both contents and contents related information (metadata) as a system does not recognize actual condition existence.

[0008]An object of this invention is to solve the above technical problems. For example, this invention is using functions, such as encryption, personal authentication, metadata, and an electronic watermark, It aims at performing right protection of contents and performing right protection of contents by accumulating, after enciphering the metadata and contents in which especially right information data etc. are stored at the transmitting side, processing re-encryption etc. by the receiver and the code's having started HDD. An object of this invention is to make right protection possible, also when viewing and listening to contents by other PDR by storing the key to encryption of contents and metadata after a viewing-and-listening contract in a personal portable CA module.

[0009]This invention is performing creation and division of metadata using the disposable key generated within the receiving terminal, and makes encryption possible for every contents. According to this invention, it aims at being made to offer service of individual specification by setting the 2nd CA module that can specify an individual.

[0010]This invention is with Lycium chinense, without putting in the owner information of contents in metadata, A contents owner enables it to specify for the first time at the time of the receipt of those who transferred contents, and it aims at realizing contents service made into the purpose of transferring the 3rd person by performing owner information entry to a CA module.

[0011]

[Means for Solving the Problem]The 2nd CA module that defined contents by metadata which is contents related information required for viewing and listening of enciphered content and its contents, and specified an individual is used for this invention. By this, offer of service to each is enabled, and security protection in delivery of contents aiming at transfer to the 3rd person is also performed, and offer

of service which transfers to the 3rd person is enabled.

[0012]Here, metadata is a general term for information other than contents fundamentally, for example, a definition can be given as contents control information, contents contents information, and contents related information. Information (EPG ()) for being the information for controlling contents by the receiving terminal side notionally, and performing stored reservation of contents, for example [Electronic Program Guide and] Information on a key of use limitation information (conditions for viewing and listening to become possible, aged 20 and over, a male, a contractor with OO broadcasting station) and a code, etc. is included at the time of a name of contents for displaying on an electronic program guide, a genre, a distribution place, and a date of scheduled distribution.

[0013]In this invention, in order to encipher every contents, separation-ization of contents related information (metadata) including information, including a viewing-and-listening contract form over enciphered content and its contents, etc., is performed. Contents are first enciphered at the transmitting side and metadata is transmitted simultaneously with enciphered contents. In a receiving terminal of a receiver which received this information, after performing processing of encryption with a disposable key generated within decryption and a receiving terminal of a transmission code in accumulation of enciphered content, and a transmission line of metadata, etc. if needed, all the accumulation of send data is performed. When viewing and listening to accumulated enciphered content, Metadata enciphered with a disposable key is decrypted, information for decoding the term of validity and contents which were copy-restricted [which were restricted and were number-of-times/ of viewing and listening /-restricted], and were enciphered, etc. are embedded, and creation and division of the metadata 1 and 2 are performed based on metadata using a disposable key again generated within a receiving terminal. It accumulates in a recording medium of a receiving terminal, etc. by considering enciphered content and metadata 2 as a set, and the remaining metadata 1 is written in user individual specific storage media, such as a CA module.

[0014]A key of enciphered content and encryption metadata is stored in a CA module after a viewing-and-listening contract. Metadata written in a user individual specific storage medium is a user individual's key, and enciphers within a CA module. When a user views and listens to contract contents, since these information was generated by the receiving terminal side, search/accounting information is reproduced based on viewing-and-listening contract information etc. within a receiving terminal. It is not necessary to encipher mass contents within a receiving terminal, and only metadata is enciphered by transmitting enciphered contents from the center side. It becomes available about information required for decoding at a decipherment of information, including these metadata. Although keys furthermore differ for every contents, all the keys of contents accumulated in a storage medium are written in a key table etc. And

a key of contents contracted [viewing-and-listening] is stored in a CA module. Although reproduction of enciphered content, etc. are performed using information on this written-in key, since a CA module etc. are needed only at the time of reproduction, it is not necessary to always install in a receiving terminal, and a viewing-and-listening contract of contents in carrying out out of homes, such as not only content purchase in a home but the exterior, is attained. A contract in the receiving terminal exterior by portability, such as a CA module, is also attained from this. Therefore, carrying of user individual specific storage media, such as a CA module, becomes possible. Enciphered content accumulated with a receiving terminal decrypts contents copied by using metadata decrypted after having copied contents enciphered at the time of a user's viewing and listening, also copying metadata enciphered similarly and decrypting copied metadata, and is reproduced. It is possible for contents data enciphered from this to be in the state where it was always accumulated, and to enjoy the same service with another CA module always. He is trying to divide into plurality of what equips with a CA module in a receiver, and a thing in which portability is possible in this invention.

[0015]

[Embodiment of the Invention]It explains according to the following titles.

1. Contents viewing other than receiving terminal which performed information 7. receiving terminal (PDR) application 8. viewing-and-listening contract used with outline 2. copyright protection method 3. ciphering system 4. receiving terminal 5.RMP6. receiving terminal (PDR) of protection of right [0016]1. Using media media, such as communication lines, such as a satellite and a land-based line, or a removable media, the integrated data distribution service shown by outline (service outline) this invention of protection of a right distributes contents to a home, and aims at performing accumulation/copy reproduction in a home in the digital state. In connection with this, the situation of infringing on the right of service providers, such as an unjust copy of data which rewrite and exceeds reproduction and private use, a copyright person, or a user, and copyright may arise. Therefore, it is necessary to protect and manage each rights, such as an owner of a copyright of contents, a broadcasting organization, and a televiewer. This invention explains supposing the data distribution which used digital satellite broadcasting as an example.

[0017](Right protection) There is the following in the copyright protection or the right protection method of contents, for example.

(1) The encryption which prevents unjust rewriting and viewing and listening of information, (2) service providers, or the user access-restriction right to the contents by a copyright person, The electronic watermark which buries information and is crowded in the metadata which is the storing format of the personal authentication for protection of the contents viewing right by a user, (3) copyright information, right information data, etc., a (4) digital picture, video, a sound, etc.

[0018]A protective method, the purpose, and the explanatory view of a function are shown in drawing 31. Here, as explaining an outline, it mentions later for details (2. refer to copyright protection method). The purposes of encryption include the unjust prevention from rewriting of information, the unjust prevention from viewing and listening of information, etc., and contents, encryption of metadata, etc. are assumed as the function. The purpose of personal authentication has [1st] protection of the user access-restriction right to the contents of a service provider and a copyright person, and checking with the user access restriction of copyright information and right information data and personal information is assumed as the function. The purpose of personal authentication has [2nd] protection of a user's contents viewing right, and access is assumed as the function by the contents in alignment with the contract information of individual units. There is [3rd] protection of privacy and access **** is assumed by personal information only the person himself/herself as the function. In addition, when distinguishing an individual and it is related to an individual, it is used for the various purpose. The purposes of metadata include use of copyright information and right information data, etc., as the function, it uses by contents and a set and storing etc. are assumed in the copyright information of the contents, and right information data. The purposes of an electronic watermark include deterrence of the unauthorized use to contents, etc., and possible ** is assumed for a use failure from application as the function at the time of the unauthorized use of contents.

[0019](System outline) The entire configuration figure of the integrated data distribution service about this invention is shown in drawing 1. The supplementary explanation figure of a whole system configuration is shown in drawing 32. A whole system is roughly divided into the transmitting side 1 which performs work of contents, distribution, etc., and the receiver 2 which comprises a receiving terminal etc.

[0020]The transmitting side 1 is provided with a transmitting center, a lock management center, a land-based line control center, a customer-relations-management center, a physical-distribution-management center, etc. As main features of the transmitting side 1, collection of information, including encryption of the contents in consideration of work of contents and pertinent information, distribution, copyright, a right, etc., lock management, a viewing history, etc., management, etc. are raised.

[0021]The receiver 2 is provided with a mobile, a cellular phone, etc. as a receiving terminal, a KIOSK terminal, a store, and other extension. As main features of a receiving terminal, possible ** is raised for the equipment of a mass storage medium for accumulating contents and pertinent information, composite of enciphered content and pertinent information and re-encryption of pertinent information, and attestation and fee collection of individual units.A KIOSK terminal is a terminal for the information guidance service set to a store, a convenience store, a public facility, etc.

If the main feature is divided into action of the transmitting side from a receiver and a receiver and is shown from the transmitting side, First, distribution of contents and pertinent information, and the key of enciphered content and pertinent information or distribution of key information is raised from the transmitting side, using satellite connection or a land-based line for example as a feature of action of a receiver. Transmission of accounting information, transmission of personal information, such as a viewing history and a request, etc. are raised from a receiver, using a land-based line as a feature of action of the transmitting side.

[0022]The transmission line 3 comprises a portable telephone network etc. as a satellite, a land-based line, a distribution channel, and other extension. From the transmitting side, the main features of a land-based line are divided into action of the transmitting side from a receiver and a receiver, and are shown. As a feature of action of a receiver, distribution of contents and pertinent information, the key of enciphered content and pertinent information or distribution of key information, etc. is raised from the transmitting side. Transmission of personal information, such as a viewing history and a request, is raised from a receiver with transmission of accounting information using a land-based line, using a land-based line as a feature of action of the transmitting side.

[0023](Processing in a whole system) The fundamental ciphering system of the whole system in the integrated data distribution service shown by this invention is shown below. First, work of contents and metadata and edit are performed in the editing system of the service provider of a sending area, a dedicated line etc. are used for a lock management center, and contents and metadata are transmitted to it. A lock management center applies the code (copyright protection code) applied in order to protect copyright to contents, manages the key, and with enciphered content, if required, it will transmit the key to a service provider. It is also considered that the key of enciphered content transmits to a receiving terminal using a land-based line, satellite connection, etc. Same processing is performed also to metadata. Encryption of contents and metadata may be performed by a service provider. Then, a code (limited reception code) is applied and distributed to for example, MPEG-2 TS which is transmission forms of contents and metadata. It is received by the receiving terminal of a receiver and the distributed data decodes a limited reception code within a receiving terminal. Then, contents and metadata are accumulated in a mass storage medium (it explains as HDD henceforth as an example), with a copyright protection code started, and it decodes in the case of viewing and listening.

[0024](Viewing and listening) About viewing and listening of contents etc., there are real-time viewing and listening and accumulated type viewing and listening, for example. Real-time viewing and listening shows that it views and listens to the contents distributed from a service provider in real time. The preexisted type broadcast only for real-time viewing and listening which assumed the receiving

terminal without a mass storage medium as real-time viewing-and-listening service, and the server-based broadcating for the accumulation service and the real-time service supposing a receiving terminal with a mass storage medium are assumed. As for the cipher system of preexisted type broadcast, the cipher system of server-based broadcating uses a limited reception code and a copyright protection code only using a limited reception code. Accumulated type viewing and listening refers to viewing and listening, after accumulating the contents distributed from a service provider in a mass storage medium.

[0025]The code gestalt in the case of accumulating preexisted type broadcast and server-based broadcating is shown below. Preexisted type broadcast is accumulated with the limited reception code at the time of transmission applied, and is made into the gestalt decoded by a limited reception code descrambler at the time of reproduction. However, since it is only a cipher system at the time of transmission, restriction may arise in services (individual contract etc.) in part. Server-based broadcating is accumulated only in the state of a copyright protection code after decoding the limited reception code at the time of transmission, and it is made into the gestalt decoded by a copyright protection code descrambler at the time of reproduction.

[0026](Real time, accumulation viewing-and-listening comparison) Comparison of real-time viewing and listening and server type viewing and listening is shown in drawing 2. This figure shows the procedure in a receiving terminal in the case of real-time viewing and listening and accumulation viewing and listening in preexisted type broadcast and server-based broadcating. This system is provided with the function which contains the limited reception code descrambler 101, the copyright protection code descrambler 103, and the decoder 104 in addition to receive section 100 and HDD102 as RMP(Rights Management & Protection)105, The copyright of contents and a right protection processing capability are shown.

[0027]In the cipher-processing procedure of real-time viewing and listening of preexisted type broadcast, after the contents received by (refer to the dotted line) and the receiver (PDR) pass along the receive section 100 and are decoded by the limited reception code descrambler 101, viewing and listening of them is attained through the decoder 104. In the cipher-processing procedure of accumulation viewing and listening of preexisted type broadcast, the contents received by (refer to the dashed line) and the receiving terminal are accumulated in HDD102, without passing along the receive section 100 and passing along the limited reception code descrambler 101. In the case of viewing and listening, it is read from HDD102, and is decoded by the limited reception code descrambler 101, and viewing and listening becomes possible through the decoder 104. The contents received by (refer to the solid line) and PDR pass by real-time viewing and listening of server-based broadcating along the receive section 100, and are decoded by the limited reception

code descrambler 101 by it. Then, after being decoded by the copyright protection code descrambler 103, viewing and listening becomes possible through the decoder 104. In accumulation viewing and listening of server-based broadcating, the contents received by (refer to the two-point ****) and PDR pass along the receive section 100, are decoded by the limited reception code descrambler 101, and are accumulated in HDD102. Then, after being read from HDD102 in the case of viewing and listening and being decoded by the copyright protection code descrambler 103, it is viewed and listened through the decoder 104.

[0028](Accumulation) Various kinds of accumulation to HDD is explained below.

(1) It has an accumulation agent function which is shown by accumulation this invention by user palatability and which makes a limited storage medium manage efficiently as one of the features of integrated data distribution service. The accumulation agent function in this service accumulates the contents in alignment with the user's taste into HDD automatically from the contents distributed. As long as the capacity of HDD allows, it is also possible to accumulate all the contents to distribute.

[0029]The user who has contracted to this channel is ability ready for receiving in a receiving terminal about the contents of all these channels. The received contents are automatically selected based on user taste, and are accumulated into HDD. From the contents in HDD, a user performs retrieval by keyword, genre retrieval, etc., and chooses, views and listens to the contents which desire viewing and listening. This system is a mechanism in which it is charged only at the contents which the user chose, out of the contents chosen and accumulated automatically.

[0030]The explanatory view of required information for a receiving terminal to judge palatability is shown in drawing 33. As processing, active processing and autonomous processing of a receiving terminal occur. In active processing, a user inputs information, including a genre, a keyword, an occupation, a hobby, etc., into a receiving terminal (those of a user with an intention). On the other hand, in autonomous processing, user's information (a viewing history, a search history, personal information, etc.) is used (with no intention of a user).

[0031](2) Accumulation EPG (Electronic Program Guide) by EPG is an electronic program guide. Using the SI information which a broadcasting station sends out, EPG constitutes program information from a receiver end, and is taken as the means of program selection. SI (Service Information) is program arrangement information. SI is the variety of information specified for the convenience of program selection. SI is defined by the postal administration ministerial ordinance again, and the contents are specified as an ARIB standard. SI is added to the extension original with an ARIB standard, and the PSI information of MPEG-2 is also contained. It is mainly used for the use of a race card display, program retrieving, and a program request to print out files. After working a race card display, program retrieving, etc., a request to print out

files (timed recording is made to HDD) of a program can be considered. As information displayed by EPG, it is thought that information, including a program title, a program subtitle, broadcasting hours, a broadcasting industry object name, the charge / free and parental existence, digital copy propriety, etc., is displayed. SI and metadata are assumed as sources of information which create EPG.

[0032](3) It is a function in which contents, such as not the accumulation by a compulsive accumulation televiewer's demand but emergency broadcast and information, are stored up more compulsorily than the transmitting side. If a receiving terminal is in content reception possible states (a power supply, an antenna, etc.), The compulsive writing which is a function in which accumulation of contents is performed without a televiewer's consent in an emergency, The periodical writing which is a function in which it decides on the usable capacity in a storage medium between a televiewer and a purveyor of service a priori, and a purveyor of service can accumulate contents without a televiewer's consent periodically if it is the range of the capacity, Under a purveyor's of service control, the storage time of contents is specified to a receiving terminal, and the time zone specification writing etc. which are the functions in which a receiving terminal accumulates contents by the specified time can be considered.

[0033]2. Explain below each protective method by the encryption, personal authentication, and metadata which were shown in copyright protection method drawing 31 in full detail.

(Encryption, RMP) In order to avoid the act which infringes on rights, such as an unjust copy of data which rewrite and exceeds reproduction and private use, and copyright, processing of viewing control, storage control, copy control, etc. is needed. The function to perform copyright of these contents and right protection processing is set to RMP (Rights Management & Protection). Each item of the metadata copyright and right information data are described to be by the personal authentication pan which performs access control to the contents of the encryption which protects contents from unjust rewriting and viewing and listening, or individual units relevant to RMP is shown below.

[0034]First, a contents cipher system is explained. Encryption of contents is indispensable in order to avoid from unjust viewing and listening of contents, a copy, and rewriting. Since the integrated data distribution service shown by this invention assumes the service accumulated in HDD in a receiving terminal, it needs to take the contents protection in HDD into consideration, and needs to encipher contents. The cipher systems used in this integrated data distribution service are a copyright protection cipher system and a restricted reception system. A copyright protection cipher system is a cipher system peculiar to this integrated data distribution service, and enciphers the contents themselves. A restricted reception system is a restricted reception system in BS digital broadcasting, and Multi2 is used for a cipher system as

an example.

[0035]The feature of a copyright protection cipher system is shown below. The copyright protection cipher system can encipher the data of contents itself not at after an assembly of the data for distribution but at the time of the completion of work of contents, and a file format is fair and it can encipher it. An encryption unit turns into a contents unit and the minimum encryption units are a resource and a stream. And it is possible to use different keys for every encryption unit.

[0036]Below, a metadata cipher system is explained. In the integrated data distribution service shown by this invention, metadata is distributed by contents and a set. Information required for [other than the search information on contents] copyright and right protection is described by metadata. Therefore, simultaneously with encryption of contents, for the copyright of contents, and right protection, encryption of metadata is also required. In that case, it is not necessary to necessarily encipher all metadata, chisel encryption processings, such as information (copyright, right information data) to be protected, are performed, and the system by which the information without the necessity for protection does not perform encryption processing is also considered.

[0037](Personal authentication) As a means of personal authentication, an individual profile is considered to be a CA module. When a CA module is carried out [personal] and an individual carries, it is considered as a user and the authentication means of a CA module, and it becomes possible by setting up an individual profile in PDR to perform attestation of a CA module and PDR.

[0038]First, a CA module is explained. A CA module is used as a means to realize personal authentication. The number of the CA modules of the former (BS/CS digital broadcasting) is one to a receiving terminal, and they are immobilization. And it becomes a viewing-and-listening contract by the family and a group unit, and a fee collection contract. With the CA module of one sheet, it becomes a viewing-and-listening contract of a receiving terminal unit, and accounting to a receiving terminal. So, in the integrated data distribution service shown by this invention, two-kind (card for CAS, card for RMP) preparation of the CA module is carried out, personal authentication is carried out, and the viewing-and-listening contract and accounting of individual units are performed. As a concrete realization means, the function related to reception of the contents which are the same functions as the conventional CA module is given to the card for CAS, and the card for RMP gives the function related to access, a viewing-and-listening contract, accounting, etc. to accumulation contents to it.

[0039]A cellular phone is made possible by individual units by giving portability to the card for RMP. The viewing-and-listening contract of individual units, accounting, etc. become possible from this thing. An IC card, SmartMedia, etc. can be considered as a CA module. After this, a CA module is explained as an IC card as an example. It is

extensible to new services, such as e-commerce, by attaching options, such as a credit function, to a CA module.

[0040]The explanatory view of the feature of the card for CAS and the card for RMP is shown in drawing 34. Into a receiving terminal, the card for CAS is always furnished and is usually used one sheet per receiving terminal. Therefore, a viewing-and-listening right unit and an accounting unit turn into a family or a group unit. The purpose of use is a restricted reception system, and accounting object things are service and an event. Therefore, a viewing-and-listening contract method serves as a prior contract. On the other hand, the card for RMP has portability, and is distributed by individual units, and an individual can carry it. Therefore, a viewing-and-listening right unit and an accounting unit turn into individual units. However, while contracting a priori per group, a group unit turns into a viewing-and-listening right unit and an accounting unit. The purpose of use is use in the whole RMP, and accounting object things are contents. The viewing-and-listening contract method in that case uses the method whose viewing and listening is attained by performing a viewing-and-listening contract.

[0041]Below, an individual profile is explained. Two or more users use a receiving terminal. In a receiving terminal, since viewing-and-listening contract in individual units, accounting, etc. are performed, whenever it uses a receiving terminal, it is necessary to change an operating environment for use users. The information for setting up environment comes to hand from a RMP card, and the area stored while using PDR is called an individual profile. The judgment (conditions, such as age and sex etc.) of the contents to which judgment of a prior contract channel and a user can view and listen as main processings based on an individual operating environment, viewing-and-listening contract processing, accounting, viewing-and-listening processing, etc. can be considered. The information used for these processings comes to hand from either the card for RMP, and an individual profile.

[0042]If the card for RMP is inserted, an individual profile will stand up and information required for an individual profile's generation will come to hand from the card for RMP. Based on the individual profile's information, the environment in a receiving terminal turns into environment for the cardholders for RMP. If a RMP card is removed, the information which came to hand from the card for RMP will be eliminated from an individual profile. When the user who is not a receiving terminal owner uses a receiving terminal, the guest profile which is a profile for guest users rises, required information comes to hand from the card for RMP like an individual profile, and it writes in a guest profile. If the card for RMP is removed, the information written down in the guest profile will be eliminated. An individual profile and the guest profile can also use the same area. Therefore, information required for individual profile generation needs to be written down in the card for RMP.

[0043](Metadata) First, if it roughly divides, right metadata and search metadata exist

in the information stored in metadata. In the integrated data distribution service shown by this invention, search, fee collection, the key information of contents, copyright information, etc. are included in metadata. Right metadata and search metadata are shown below.

[0044]First, right metadata is explained. Right metadata is metadata the information in connection with copyright or a right is described to be. The information concerned is used for copyright protection. The main items of right metadata are shown below.

[0045](1) It is information including the information on the existence of the information code about a cipher system, the cipher system currently used, and a key, etc., and is the information enciphered in part. Information, including a cipher system, key information, etc., may be rewritten within RMP. The main items are shown below.

- The existence and the key of the cipher system and code of the cipher system and metadata of contents, or key information [0046](2) It is information including the information about the copyright of information content about a right, and is the information which is fixed at the time of broadcast and enciphered altogether. The main items are shown below.

- A right holder, an applicable law, and a management place [0047](3) Contract information (granted information)

It is information including the utilization condition etc. which a screen should be shown at the time of a viewing-and-listening contract, and is the information which is fixed at the time of broadcast and enciphered altogether. The main items are shown below.

- Copy permission / accumulation permission, the age limit, the term of validity, and a fee [0048](4) It is information including the information which is needed at the time of accounting information accounting, and is the information which information is written in in part at the time of a viewing-and-listening contract, and is enciphered altogether. The main items are shown below.

- A charging method and an accounting state [0049](5) At the time of a personal authentication information viewing-and-listening contract, it is the information used when the personal authentication at the time of accumulation, etc. is required, and is the information which information is written in and enciphered in part from the card for RMP, and a profile within RMP. The main items are shown below.

- A user's individual ID, age, and sex [0050](6) It is the information which is needed when performing information storage about a using state, and protection to the copied contents, and for the information which is written by a user's use each time and replaced, in order to protect from a data alteration and an unauthorized use, it is enciphered altogether. The main items are shown below.

- The accumulation utilization time, using frequency, and viewing-and-listening time [0051](7) It is the information which is needed when accumulating information content about accumulation, and metadata, and a part is rewritten at the time of accumulation, etc. The main items are shown below.

- Specification and an accumulating method of a storage place [0052]Below, search metadata is explained. Search metadata is metadata the information in connection with search is described to be. The information concerned is used for retrieval processing. However, depending on a search engine, the information on right metadata may be used as search information. The main items of search metadata are shown below.

[0053](1) It is the information for distinguishing from contents besides the attribution information of the contents themselves, and metadata, and is the information fixed at the time of broadcast. The main items are shown below.

- Existence of content ID, a contents name, and the charge [0054](2) It is the information expressing the attribution information program / service of a program/service, and include the information stored in a retrieving table. It is the information fixed at the time of broadcast. The main items are shown below.

- A program name, a channel name, a keyword, an outline, and a broadcasting organization code [0055]3. There are a copyright protection cipher system and a restricted reception system in the cipher system of the integrated data distribution service shown by ciphering system (cipher system) this invention. The explanatory view of the contents enciphered in the transmitting side and the code gestalt of metadata is shown in drawing 3. First, at the time of the end of work of contents and metadata, contents are used per a file or stream, key Kk 110 is used in a copyright protection code, and it enciphers. The key is embedded at metadata and they are 111 metadata files with a copyright protection code Key Kw2 It enciphers using 112. MPEG-2 TS which is transmission forms of these enciphered content and encryption metadata is enciphered by key Ks 113.

[0056](Key distribution system) Transmission of an image stream is explained first. Generally, an image stream is blocked by fixed-length data. Header information is added to each block. TSP (Transport Stream Packet) is a group of this header and data, and points out the format of the data packet at the time of transmission. A data part is enciphered when hanging scramble (code) with a preexisted type. ECM (Entitlement Control Message) is information transmitted to the whole user in common, and is a transmission message of common information including program information and control information. Program information is a key for the information about a program, and descrambling, etc., for example, and control information is instructions of the forcible ON/OFF of the descrambling function of a decoder, etc., for example. ECM is not the information which is transmitted with contents, and is limited and sent to a certain specific user in order to transmit the scramble key of contents fundamentally. EMM (Entitlement Management Message) is a transmission message of the individual information containing the work key for solving the code of the contract information for every member, and common information. EMM is information which limits a certain specific user and is sent in order to send an

entrepreneur's key etc. which the user made a contract of fundamentally. CA(Conditional Access) system is a system which points out a restricted reception system and controls service (organization channel) and viewing and listening of an event (program) by an enciphering key. Below, the distribution method of the encryption data and the key of a restricted reception system and a copyright protection cipher system is shown.

[0057](Restricted reception system) The encryption data of BS transmission-line code and the transmission method of a key are shown in drawing 4. First, it enciphers with the scramble key Ks to the TS packet which is transmission forms of the event having contained contents, metadata, etc. Next, the scramble key Ks is enciphered by work key Kw1, and key Ks' is created. Work key Kw1 at this time is a key defined for every entrepreneur of a broadcast side, and it is a key concerned possible [viewing and listening of this service], and improper. Finally work key Kw1 is enciphered for every receiving terminal by personal key Km1 which is a meaning, and key Kw1' is created. As for encryption event data, BS transmission line and key Ks' use these enciphered data and a key, ECM and key Kw1' uses EMM, and it transmits. The receiving terminal which received these encryption data is decoded using personal key Km1 stored in CA module 1. First, key Kw1' transmitted by EMM is decoded using personal key Km1, and work key Kw1 comes to hand. Next, Ks' transmitted using ECM is decoded using work key Kw1, and the scramble key Ks comes to hand. Finally the encryption event data which used BS transmission line and was transmitted is decoded using the scramble key Ks, and the TS packet which is transmission forms of an event comes to hand.

[0058](Copyright protection cipher system) The contents in the case of using metadata for drawing 5 and transmitting the contents key Kk to it and the transmission method of metadata are shown. First, contents are enciphered with the contents key Kk. The contents key Kk can use different keys for every contents. However, it is common to the set with each service provider, or an altogether common thing is also possible. The contents key Kk is added to metadata, and metadata is enciphered by work key Kw2. Work key Kw2 at this time uses different keys for every set with each service provider, or an altogether common thing is also possible for it. And it is also possible to use key Kw1 used in BS transmission-line code. Finally, work key Kw2 is enciphered with the key Kmc common to a meaning or all for every receiving terminal, and key Kw2' is created. Enciphered content and encryption metadata transmit these enciphered data and a key using BS transmission line, and key Kw2' is transmitted using EMM. The receiving terminal which received these encryption data is decoded using the key Kmc stored in the receiving terminal. First, key Kw2' transmitted by EMM is decoded using the key Kmc, and work key Kw2 comes to hand. Next, the encryption metadata transmitted using BS transmission line is decoded using work key Kw2, and metadata comes to hand. Finally the enciphered

content which used BS transmission line and was transmitted is decoded using the contents key Kk as which metadata is filled in, and contents come to hand.

[0059](Cipher-processing procedure) The outline of cipher processing in this service is shown below. In order to perform copyright of the contents in a storage medium and in portability, and right protection, at the transmitting side, contents are enciphered, the key is stored in metadata, metadata is enciphered with a different key, and it distributes by enciphered content and an encryption metadata set. First, the enciphered content and encryption metadata which were received by the receiving terminal decode encryption metadata, and hold it to the key table which obtained the key Kk of contents and in which the security in a receiving terminal was protected. Next, metadata is re-enciphered with the same key as contents, and enciphered content and encryption metadata are accumulated in HDD. If viewing-and-listening contents are chosen, metadata will be read from HDD, and a key will be come to hand and decoded from a key table. A viewing-and-listening contract is performed after that, and the key of contents and metadata is stored in a personal portable CA module. By storing a key in a personal CA module, viewing and listening of contents becomes possible also for other receiving terminals. After all the processings finish, enciphered content is decoded using the key of contents and viewing and listening becomes possible.

[0060]The cipher-processing procedure in a whole system is concretely shown below using a flow chart. Respectively, drawing 6 is an enciphering procedure of the transmitting side, drawing 7 is a distribution procedure of the transmitting side, and drawing 8 is a flow chart which shows a receiver procedure.

[0061]First, the enciphering procedure of the transmitting side of drawing 6 is shown. A copyright protection code is applied first. First, the file and stream which constitute contents are enciphered with the key Kk per a file basis or stream (120). Under the present circumstances, the file within a contents unit uses the same key Kk. And the key Kk of enciphered content is stored in metadata (121), and metadata is enciphered by key Kw2 (122). Next, a limited reception code is applied. Contents and metadata are encoded to MPEG-2 TS which is a transmission format (123), and the pay load of a TS packet (TSP) is enciphered with the key Ks (124).

[0062]Next, the distribution procedure of the transmitting side of drawing 7 is shown. Work key Kw2 is enciphered with the key Kmc a priori, and it distributes, using EMM as key Kw2' (125). Similarly, work key Kw1 is enciphered by personal key Km1, and individual distribution is carried out a priori, using EMM as key Kw1' (126). Then, the event enciphered by broadcasting hours with the key Ks is distributed (127). And it enciphers by work key Kw1 and the key Ks is distributed using ECM (128).

[0063]Next, the receiver procedure of drawing 8 is shown. A restricted reception system is processed first. Key Kw1 enciphered is decoded using personal key Km1 in the card for CAS (CA module 1), and key Kw1 comes to hand (129). And the

encryption Ks is decoded by key Kw1 and the key Ks comes to hand (130). An encryption event is decoded with the key Ks and an event comes to hand (131). Next, a copyright protection cipher system is processed. First, Kw2 enciphered is decoded using the personal key Kmc stored by the default in PDR a priori, and key Kw2 comes to hand (132). Although the personal key Kmc is a key currently prepared in the card for RMP (CA module 2) by the default, updating by a lock management center etc. is also possible. Next, encryption metadata is decoded by key Kw2 (133), and the key Kk comes to hand (134). And metadata is enciphered with the key Kk (135) and it accumulates in HDD (136). Enciphered content is accumulated in HDD as it is. The key Kk is held to the key table in which the security in a receiver was protected. Then, if a user chooses the contents which desire viewing and listening, encryption metadata will be read from HDD (137) and it will decode using the key Kk currently held at the key table (138). Viewing-and-listening contract information is filled in after a viewing-and-listening contract, and with the card for RMP, a part of metadata (viewing-and-listening contract information, the key Kk, etc.) is stored in a whole profile, if required (139). Viewing-and-listening contract information is information in connection with viewing and listening, the contract, and fee collection of contents, including contract content ID, contract time, conditions of contract, accounting information, etc. If a viewing-and-listening contract and the processing in connection with metadata finish, enciphered content will be read from HDD and it will decode using the key Kk (140).

[0064]Here, the main features in cipher processing of contents are shown below. It enciphers and distributes [1st] with the key Kk using a copyright protection cipher system at the transmitting side. It is accumulated in HDD, with the copyright protection code started which is the same cipher system as the cipher system applied [2nd] at the transmitting side. That is, enciphered content is enciphered with the key Kk. After a viewing-and-listening contract finishes with the 3rd, a copyright protection code is decoded using the key Kk.

[0065]The feature in metadata cipher processing is shown below. It enciphers and distributes [1st] at the transmitting side by key Kw2 which is a work key of a copyright protection cipher system. Since the key Kk of a copyright protection cipher system is filled in into metadata, metadata is enciphered using the work key of a copyright protection cipher system. If received [2nd] by the receiving terminal, after decoding Kw2 and extracting required information, it is accumulated in HDD after a re-code with the contents key Kk. The reason which is not accumulated in HDD while it had been enciphered by key Kw2, Since that two or more metadata enciphered with the same key will exist, and intensity becomes weak to an attack key Kw2 since it is only to a broadcasting industry object during fixed time, and key Kw2 are changed periodically, As long as the metadata concerned exists, after change has a reason for holding key Kw2 of the past, etc.

[0066]4. The basic constitution figure of a receiving terminal is shown in receiving terminal drawing 9. The receive section 203 which receives various data, such as PSI/SI whose receiving terminals are 20 (PDR), contents, metadata, and program arrangement information, DEMUX204 which returns the data multiplexed by MUX of the transmitting side to the state before multiplexing at a series of data, The mass storage medium (HDD etc.) 205 which stores the received data of contents, metadata, etc., the IC card of the former (BS/CS digital broadcasting) which stores information required when performing processing related to a restricted reception system -- or, The card 201 for CAS supposing the chip provided with the function (CA module 1), Portability is given and it carries individually, and when processing personal authentication, a viewing-and-listening contract, etc., it has the card 202 (CA module 2) for RMP which stores required information, the copyright of contents, and the RMP200 grade which is right protection functions.

[0067]The functional block diagram in PDR is shown in drawing 10. In a real-time type, it is received by the reception 210, and preexisted type broadcast contents decode the code of the restricted reception system (CAS) 211, and are reproduced in real time. Next, an accumulated type shows processing of server-based broadcating contents. First, the taste application 216 judges a user's taste based on the information inputted by the user interface, viewing history information, etc. The information inputted into the palatability application 216 has a hobby, special ability, etc., for example as a viewing history as inputs by a user interface, such as a genre of viewing-and-listening contents, and a keyword. The palatability application 216 creates user palatability information from the above-mentioned information. Then, after being attested from RMP212, an EPG table, a retrieving table, etc. which are accumulated in some area in HDD213 which becomes accessible are seen, and the contents which suited the user's taste are selected. User palatability information is created in the format which met the genre and keyword of contents. When creating user palatability information, the word with much number of times of an appearance sets up a priority highly. A genre, a keyword, etc. of each EPG information by which the palatability application 216 is furthermore stored in the EPG table, The created user palatability information is compared (it is a deed about search), it considers that congruous (ambiguous coincidence) contents are the contents in alignment with user palatability, and stored reservation (from contents with a high priority of palatability to stored reservation) is carried out. The contents of HDD214, metadata, etc. cannot be accessed from the palatability application 216. On the other hand, it is accessible from the palatability application 216 in the EPG table of HDD213, a retrieving table, etc. It is also possible to set a priority also to the user taste and to select from contents with a higher priority preferentially. As opposed to the function to construct one selected by the palatability application 216 grade or the timed recording schedule of two or more contents as schedule management, and to perform reception 210 according to the

schedule, Information required for reception of ID of contents, ID of metadata, broadcasting hours, etc. is passed. The information of reservation of picture recording is beforehand passed from the broadcasting hours of contents, or taste application judges to the broadcasting hours of contents, and the timing by which the taste application 216 advances request to receipt to reception 210 function can also take out recording directions to them. When the taste application 216 constructs a schedule, how to construct a schedule by the number of the tuner which exists in PDR changes. That is because the number of the contents which can be accumulated in HDD changes simultaneously corresponding to the number of a tuner, for example, if two or more tuners exist in PDR, accumulation of two or more contents of it will be attained simultaneously, and it will become possible to carry out scheduling of the contents duplicate in time. Based on the schedule information passed from the taste application 216, reception 210 function performs accumulation processing of contents and metadata. First, it is judged whether by a schedule, the metadata out of which accumulation directions have come can be acquired by RMP212, encryption metadata can be decoded there, and it can accumulate based on information, including right information data etc., required at the time of accumulation. When it judges that accumulation is possible, after reading the contents of a set into RMP212 and re-enciphering metadata from the information on metadata, contents and metadata are accumulated in HDD214. Then, when a user chooses viewing-and-listening contents, metadata is first read into RMP215 and viewing-and-listening contract processing, accounting, etc. are performed there. Then, contents are read into RMP215, and it becomes reproduction of contents after decoding by RMP215.

[0068]5. The lineblock diagram of cipher processing in RMP is shown in RMP (cipher processing in RMP) drawing 11. As for the cipher system in this integrated data distribution service, a restricted reception system and a copyright protection cipher system are assumed. As an example, cipher processing of the cipher system which has required the limited reception code and the copyright protection code, and the cipher system which has required only the copyright protection code is shown. When the limited reception code and the copyright protection code have started, after contents passed along the receive section and they are decoded by the limited reception code descrambler 250, they are accumulated in HDD251. If a user determines viewing-and-listening contents, after being decoded by the copyright protection code descrambler 252, a decoder will be reproduced and viewing and listening will become possible. Only in the case of a copyright protection code, after contents pass along a receive section, they are accumulated in HDD251. And if a user determines viewing-and-listening contents, after being decoded by the copyright protection code descrambler 252, a decoder will be reproduced and viewing and listening will become possible.

[0069](Function of RMP) Each function in RMP is shown below. A RMP controller, a

reception control, storage control, copy control, viewing control, Functions, such as fee collection control, encryption, decryption, personal authentication control, time of day control, viewing history control, external instrument attestation, communications control, search control, Plug In application attestation control, metadata control, profile control, IC card control, and key control, can be considered.

[0070]The functional constitution figure in RMP is shown in drawing 12. Each function is explained below. A RMP controller is a function which carries out control management of the processing etc. which are performed inside RMP. The main function is control management (control) of I/feed function with the RMP exterior, and each function inside RMP(s) (a decoder, application, a control manager, etc.), etc. A reception control is the function to judge the classification of service, etc. and to perform selection of the decoding processing inside RMP, etc. from PSI/SI and metadata which were acquired. The main functions are generation etc. about the information added [PSI/SI / PSI/SI] to metadata from PSI/SI with selection of contents and the acquisition course of metadata selection of the decoding processing of contents and metadata, and if needed.

[0071]Storage control is a function which controls the accumulation operation to storage media by which it is generated inside RMP, such as contents and metadata, by the information on metadata and a profile. The main functions are [whether accumulation directions (reservation of picture recording etc.) of contents have come out from the information on a whole profile or contents can be accumulated from a judgment and the information on metadata, and] the accumulation directions to the storage medium of a judgment, and contents and metadata, etc. Copy control is a function which controls the copy demand generated by user requests, such as a viewing-and-listening contract, etc. by the information on metadata. The main functions are [whether the copy of contents is more possible than the information on metadata, and] copy directions of judgment, and contents (Kk) and contents (Ks) **, etc.

[0072]Viewing control is a function which controls reproduction of the contents within RMP from the copyright of metadata, right information data, etc. to a user's viewing-and-listening demand. The main functions by comparison of the copyright of metadata, and right information data and the personal information on the card for RMP. A user by comparison of accessible contents, or a judgment, the copyright of metadata and right information data and user request information. They are contents to which a user can view and listen, a judgment and the viewing-and-listening contract processing of contents, generation of viewing information and contract information, and matching of RMP and reproduction application. Fee collection control is a function which controls by the conditions of contract in metadata, and a user's conditions-of-contract selection the accounting which happens by a viewing-and-listening contract etc. The main functions are accounting, generation of

accounting information, etc. based on contract information.

[0073]An enciphering function is a function which controls encryption of the metadata inside a receiving terminal. The main functions are encryption of metadata, etc. A decoding function is a function which controls the contents inside RMP, and decryption of metadata. The main functions are decoding of a restricted reception system code, decoding of a copyright protection code (enciphered content, encryption metadata), etc.

[0074]A personal authentication function is a function to perform attestation between a user, the card for RMP, and an individual profile. By the main functions' inserting an IC card in a receiving terminal, and entering a password, It is a user's discernment etc. by the card for RMP, an individual profile's attestation, and the password in an individual profile a user, attestation of the card for RMP, and by inserting the card for RMP in a receiving terminal. Time of day control is a function for showing exact time (the alteration of the time information by a user, etc. are prevented) in the check of the term of validity at the time of contents decoding, etc. The main functions are shown below. From information, including TOT etc., it is unified management etc. about amendment of time, and the current time in a receiving terminal. Therefore, it also becomes possible for it to become unnecessary for a user to set up time and not to prepare the user interface of time setting out, and the protection of the right about time, such as the term of validity, of it by change of the time information on purpose by a user etc. is attained. The time information itself, such as TOT, may be enciphered and distributed.

[0075]Viewing history control is a function which generates a viewing history and palatability information from the viewing information stored in the individual profile. The main functions are [viewing information / of an individual profile] creation etc. about user palatability information from creation and viewing history information in viewing history information. When an external instrument authentication function connects an external instrument for the purpose, such as accumulation, a copy, and reproduction, it is a function to identify the copyright protection level of the external instrument, inaccurate apparatus, etc. The main functions are attestation of the copyright protection function of an external instrument, etc. based on the information in metadata.

[0076]Communications control is the function to perform control about the safety of the channel at the time of using external lines, such as viewing history collection and accounting information collection, and transmitting and receiving the data in connection with copyright or privacy. The line control which the main functions perform circuit terminations, such as RMP and a modem, and ensures connection and cutting of a circuit, When the error of the data by which it may be generated in the middle of the synchronous control and the data communications which are between transmission and reception and scramble for a synchronization is checked and an

error is discovered, they are transmission control, such as error control which corrects it, the authenticating processing using a public key system, etc. Search control is search of the specified data in a storage medium, and a function read into RMP. The main functions are reading target contents or metadata from the inside of HDD or a removable media, etc. in RMP at the time of removable media accumulation, etc. at the time of viewing and listening at the time of a viewing-and-listening contract at the time of search.

[0077]Plug In application attestation control is a function which is attested with the application [Plug In / application / PDR] and only the accepted application makes accessible with RMP. The main functions are the authenticating processings of Plug In application, etc. Metadata control is a function which controls extraction of the data which is needed to metadata when performing each processing of the reception within RMP, accumulation processing, etc., and storing of the information generated at the time of each processing. The main functions are storing, division of metadata, etc. in the applicable portion of metadata about the information generated by extraction, reception, viewing-and-listening processing, etc. from metadata in the information which is needed when performing each processing of accumulation processing, viewing-and-listening contract processing, retrieval processing, etc.

[0078]Extraction from the profile of the data which is needed when managing a whole profile and an individual profile and performing each processing in RMP with profile control, It is a function which controls storing (the user configuration in the receiving terminal using information, including EMM2, the IC card for RMP, etc., etc. are included) in the profile of the generated information. The main functions are [contract information / of an individual contract and a whole contract] managements etc. in personal information, such as management, individual ID, group ID, about management, management of viewing history information, and the schedule of reservation of picture recording etc. IC card control is a function which controls access to the card for CAS in each processing, and the card for RMP. The main functions have personal authentication etc. in the card for CAS in the information on EMM1 and ECM1 from storing directions, **** directions of the card for CAS to the scramble key Ks, and the personal information on the card for RMP. Key control is a function which generates [key] inside RMP and controls lock management. The main functions are control of a key table, etc.

6. Information used with receiving terminal (PDR) [0079]The integrated data distribution service shown by this invention, Using personal portable CA module 2, the concept of individuals, such as a viewing-and-listening contract of individual units, and accounting, The service which carried CA module 2 and had a concept of portability, such as transmission of the content purchase in a KIOSK terminal, the payment of a fee, and viewing history information and viewing and listening of the contents in other receiving terminals, is assumed. Therefore, the information which

should always be stored in a receiving terminal, and the information by which portability should be carried out exist.

[0080]Information required in the case of processing of RMP is metadata, a whole profile, a key table, a card for CAS, a card for RMP, a retrieving table, etc. These each information is explained below. There is an individual profile's concept of being used in order to set PDR as personal environment besides the above, and the information obtains information required from the card for RMP whenever a user inserts RMP, and generates an individual profile. However, it is also possible for required information to come to hand from the card for RMP at any time, without preparing an individual profile. PDR constants are a whole profile, a key table, a card for CAS, a retrieving table, etc. The information in which portability is more possible than PDR is a card for RMP, etc.

[0081](Card for CAS (CA card 1)) The explanatory view of the information which needs to be made to always fix to PDR is shown in drawing 35. That is, the information which it was new to drawing 35 (A) in the right protection system of this invention, and was added to it is shown, and the information used for drawing 35 (B) as an object for limited reception in the digital broadcasting of the former (BS digital broadcasting of December, 2000 to service yne) is shown. These are information stored by immobilization in a receiving terminal. Thus, since the card for CAS stores the same information as the IC card for CAS of BS broadcasting, the information about reception of contents, etc. are stored.

[0082](Card for RMP (CA card 2)) The explanatory view of the information which can carry out portability from PDR is shown in drawing 36. This is information stored in the card for RMP with the portability which is a new concept in the right protection system of this invention. Thus, the card for RMP is prepared for every user using a receiving terminal, and individual information, the viewing-and-listening contract information of contracted contents, etc. are stored. If the card for RMP is inserted in a receiving terminal, required information indicated to the whole profile, such as viewing-and-listening contract information of the contracted contents by the group member in a group contract, will be written down in the card for RMP. Then, in order to make the inside of a receiving terminal into a user individual's environment, the required information in the card for RMP is read in RMP, and it develops to an individual profile. However, it is also possible to access the card for RMP at any time, and for information to come to hand, without developing to an individual profile.

[0083](Metadata) Processing **** of RMP of the metadata the pertinent information on contents is indicated to be is indispensable. The disposal method for contents changes seeing copyright, right information data, etc. which have been indicated to metadata. The information which the information indicated to this metadata should apply a code, and should be kept is also included. The details of metadata are as above-mentioned.

[0084](Whole profile) The explanatory view of the main items of a whole profile and the contents is shown in drawing 37. The PDR setup information etc. which are the group information which summarized the information about the schedule of the terminal information in connection with the whole user who mainly uses a receiving terminal, the stored reservation of contents, a viewing-and-listening request to print out files, etc., and the individual's information are stored.

[0085](A key table and a retrieving table) The explanatory view about the contents of a key table and the retrieving table is shown in drawing 38. The information on the key which carries out storage management of the key table inside a receiving terminal like drawing 38 (A), etc. are stored. In it, key Kw2, Kk, and three kinds for Kmc exist. However, to a receiving terminal, since it is common to only or all the receiving terminals, the key Kmc stores only a key and the very thing. The information which is needed when a retrieving table identifies the storage place of contents and metadata in each processing like drawing 38 (B) is stored. An outline is used if needed from problems, such as capacity.

[0086](The function of RMP, and the relation of information) Each function of RMP and an example of the relation figure of information area used in that case are shown in drawing 39. Such a relation is not necessarily realized and an exception may arise with each procedure. For example, metadata and a whole profile are used in ** storage control, and metadata, an individual profile, and the CA card 2 (card for RMP) are used in ** viewing control.

[0087]7. Explain each application about PDR below to receiving terminal (PDR) application.

(Retrieval application) Retrieval application has a function which helps the time of choosing the contents which desire viewing and listening from the contents accumulated in the storage device in accumulation viewing and listening. The information about each contents for performing retrieval processing comes to hand from a retrieving table and metadata. RMP is passed, RMP accesses a storage device and the contents information (the location of contents, the location of metadata, etc.) with selected retrieval processing reads data in RMP. Not only the contents chisel accumulated in storage media, such as HDD, but a retrieval object can be searched by the contents information of the schedule distributed in the future coming to hand. It is also possible for the information distributed as an object for EPG to come to hand as an example, to refer to a keyword, a title, a genre, etc., and to perform reservation of picture recording.

[0088](Primitive operation procedure) The primitive operation flow chart from content reception to viewing and listening in a receiving terminal is shown in drawing 13. Procedure Reception (S1301), the decoding processing of a limited reception code (S1303), It is carried out in order of accumulation processing (S1305), retrieval processing (S1307), viewing-and-listening contract processing (S1309), accounting

(S1311), metadata processing (S1313), and contents decoding processing (S1315). Each processing is explained in detail below.

[0089](S1301, reception) The procedure of reception, the cipher system at the time of distribution, and the relation of the code gestalt at the time of accumulation are shown in drawing 14. The following cases can be considered as a cipher system of the distributed data.

CASE -- 1:restricted reception system + copyright protection cipher system CASE2:restricted reception system CASE3:copyright protection cipher system CASE4: -- with no encryption [0090]When a receiving terminal receives contents, the code gestalt at the time of HDD accumulation is recognized, and the decoding processing procedure in each case is chosen. The code-less accumulation accumulated in the state where it is not enciphered as the restricted reception system accumulation accumulated as a code gestalt at the time of accumulation of contents applying a restricted reception system to contents and the copyright protection cipher system accumulated in the state where contents are enciphered in the copyright protection code can be considered.

[0091](Decoding processing of S1303 and a limited reception code) The decoding processing procedure of a transmission-line code is shown in drawing 15. It decodes according to the decoding processing procedure identified by the reception-control function. The decoding processing procedure in the case of a cipher system is shown below at the time of each accumulation.

- Restricted reception system accumulation : only metadata decodes a limited reception code.

- copyright protection cipher system accumulation: -- CASE1: -- limited reception code decoding of both contents and metadata

CASE3: - code[processing-less]-less accumulation: Contents, limited reception code decoding of both metadata

[0092](S1305, accumulation processing) The procedure of accumulation processing is shown in drawing 16 and drawing 17. In this step, after decoding a transmission-line code, it processes until it accumulates in HDD. The main procedure is shown below.

- They are key Kk acquisition 302 and the metadata encryption 303 from entry 301 and metadata in search of metadata, and a part of right information data to metadata decoding 300 and a retrieving table. [0093](S1307, retrieval processing) The procedure of retrieval processing is shown in drawing 18 and drawing 19. Retrieval processing is processing at the time of choosing the contents accumulated in viewing and listening or a removable media. 311 to which the retrieval application which is the application of a receiving terminal performs retrieval processing, and the viewing control of RMP performs reading of the data into 310 and RMP from HDD. The contents in HDD are searched by a user request, and search results are shown. The contents to show are made into two steps with a detailed degree as follows.

** In the information on a retrieving table, it is the detailed information of the detailed contents of the program, a fee, etc. by the information on outlined information ** metadata, such as a title of contents, and a program summary. [0094](S1309, viewing-and-listening contract processing) The procedure of viewing-and-listening contract processing is shown in drawing 20. Viewing-and-listening contract processing is performed based on the information inputted and checked on the occasion of a user's viewing-and-listening contract of contents. 321, 322 which present the contract information of metadata to a user and judge whether contents viewing is possible for the user in consideration of 320, the right to access, a viewing condition, etc.

[0095](S1311, accounting) The procedure of accounting is shown in drawing 21. Here, based on contract information, accounting is performed to the contents which performed the viewing-and-listening contract. 331 stored in a whole profile if the accounting information which is information on an accounting result, viewing information, contract information, and the viewing-and-listening contract information that summarized accounting information are required.

[0096](S1313, metadata processing) The procedure of metadata processing is shown in drawing 22. Here, after processings in connection with a contract, such as viewing-and-listening contract processing and accounting, end, the viewing-and-listening contract information which summarized those information is written down in metadata, and processing treatment of the metadata is carried out. The main procedure is shown below.

- If it is storing 341 and necessity in entry 340 and viewing-and-listening contract information, Kk, etc. about viewing-and-listening contract information in metadata at a RMP card, it is the encryption 342 at key Km2 about the inside of a RMP card.

[0097](S1315, contents decoding processing) The procedure of contents decoding processing is shown in drawing 23 and drawing 24. Here, the enciphered contents are decoded when viewing and listening to the contents to which the viewing-and-listening contract was performed. The key Kk of the contents code is stored in the individual profile. The key Kk comes to hand and the procedure which decodes contents is shown below.

- It is the contents decoding 352 in HDD about the metadata in HDD at Kk of judgment 351 and the individual profile of decoding 350 and user restrictions with an individual profile's key Kk generated from the card information for RMP.

[0098](Accumulation in the contents key transmission model using metadata) The explanatory view of the procedure in the contents key transmission system which used metadata is shown in drawing 43. The flow chart of the procedure in a contents key transmission system is shown in drawing 44. The procedure in the contents key transmission system which used metadata for below is explained. First, BS transmission-line scramble is decoded using Ks, Kw1, and Km1 that are accumulated

in CA module 1 (500), and the enciphered content 401 and the encryption metadata 451 come to hand. In this case, the contents key Kk is contained in the encryption metadata 451. Next, the metadata 451 is decoded using work key Kw2 which is beforehand transmitted to the receiving terminal (PDR) 3, and is stored in RAM452 in a code / decryption module (503,453), The information used for retrieval processings, such as search/accounting information indicated to metadata, is extracted, and it adds to the retrieving table 410 (504). Search/accounting information of the contents 406 in HDD4 are indicated, and when this retrieving table 410 searches, it is used.After extracting the information used for retrieval processing from metadata and adding a postscript to a retrieving table, The metadata 405 which set to key Kt453 the value Kt made to generate or prepare within a code / decryption module (506), carried out metadata once decoded by Kw2 re-encryption 453 by Kt (507), and was enciphered by Kt is generated (453). The key Kt is stored in RAM452 in a code / decryption module. This key Kt decodes the metadata 451 before HDD4 accumulation, and is a key made to generate or prepare within a code / decryption module whenever it carries out re-encryption 453. Then, the encryption metadata 405 enciphered with the enciphered content 406 enciphered with the contents key Kk and the key Kt is accumulated in HDD4 by a set (508). It is good also as a key different every metadata 414.

[0099](Contents storage to a removable media) The flow chart of the contents storage procedure to a removable media is shown in drawing 45. Below, procedure until it accumulates the contents 406 accumulated in HDD4 in the removable media 5 is explained. With reference to drawing 43, the contents storage processing to a removable media is explained.

[0100]When a user inputs a keyword etc., retrieval processing 412 in HDD4 is performed based on the information on the retrieving table 410 (520). A user chooses the accumulation contents 409 from the search results (520). And the metadata 408 to the selected contents 409 is copied to the work area in the receiving terminal (PDR) 3. Copied metadata 408 is carried out decoding 413 using the key Kt (522). And a user accumulates determination 415 by adding required information after checking the conditions of contract of the selected contents 408 (523). In response to operation of a user's accumulation determination, accounting 416 is performed from the conditions of contract which the user made a contract of (524). The contract information of the metadata 414 is created from the result of conditions of contract and accounting (525). Then, the metadata 414 is divided into the metadata 1 and 2 (526). And value Kt' made to generate or prepare within the receiving terminal (PDR) 3 is set to key Kt'418 (527). This key Kt' is a key made to generate or prepare within the receiving terminal (PDR) 3 whenever it enciphers before accumulating the metadata 2 in the removable media 5 and HDD4 grade after the viewing-and-listening procedure of the contents 409. The metadata 2 is enciphered by key Kt' (528), and it

accumulates in the removable media 5 (529). Next, the information about key Kt' or a key is written down in the metadata 1. The transmission line where security is protected in the metadata 1 is used, and it is CA module 2. It accumulates in 101 (531) and is CA module 2. Personal key Km2 accumulated in 101 It takes encryption 422 using 424 (530). The transmission line where security is protected is used in this processing, and it is personal key Km2. 424 is inputted in the receiving terminal (PDR) 3, CA module 2 after enciphering the metadata 1 include the information about key Kt' or key Kt' using personal key Km2424 (422, 530) Accumulating in 101 (531) is also possible. As methods other than this, security may transmit the metadata 1 include the information about key Kt' or key Kt' to CA module 2101, and may save it as it is in the kept transmission line. If all processings about the metadata 414 are completed, the enciphered content 409 will be accumulated in the removable media 5 (532). Thus, metadata 2 which the information stored in a removable media is enciphered by key Kk', and contains the key Kk It becomes the contents 427 enciphered with 421 and the key Kk.

[0101](Contents viewing) The flow chart of contents viewing procedure is shown in drawing 46. The explanatory view about the data flow of after-accumulation viewing and listening which used metadata is shown in drawing 47. Below, procedure until it views and listens to the contents 408 accumulated in HDD4 with reference to drawing 43 is explained. Metadata and enciphered content are booked in the code which contains the key Kk in HDD4. When a user inputs a keyword etc., retrieval processing 412 in HDD4 is performed based on the information on the retrieving table 410 (520). A user chooses the viewing-and-listening contents 409 from the search results (540). And the metadata 408 to the selected contents 409 is copied to the work area in the receiving terminal (PDR) 3.

[0102]Metadata is processed as follows. Copied metadata 408 is carried out decoding 413 using the key Kt (522). And viewing and listening is carried out determination 415 after a user's checking the conditions of contract of the selected contents 409 (541). Accounting 416 is performed in response to operation of a user's viewing-and-listening determination from the conditions of contract which the user checked and made a contract of (524). Contract information of metadata is carried out creation 417 [result / of conditions of contract and accounting] (525). Then, the metadata 414 is divided into the metadata 1 and 2 (526). And value Kt' made to generate or prepare within the receiving terminal (PDR) 3 is made into key Kt' (527). This key Kt' is a key made to generate or prepare within the receiving terminal (PDR) 3 whenever it enciphers before accumulating the metadata 414 in the removable media 5 and HDD4 grade after the viewing-and-listening procedure of the contents 409 (good [as a key different every metadata 414] in addition). Next, metadata 2 is carried out encryption 419 by key Kt' (528), and it accumulates in HDD (542). Next, the transmission line where security is protected is used and it is personal key Km2.

424 is inputted in the receiving terminal (PDR) 3, It is the metadata 1 including the information about key Kt' or key Kt' Personal key Km2 CA module 2 after taking encryption 422 using 424 (530) It accumulates in 101 (531). In this processing, the information about key Kt' or key Kt' is written down in the metadata 1. The transmission line where security is protected in the metadata 1 is used, and it is CA module 2. It accumulates in 101 (531) and is CA module 2. Personal key Km2 accumulated in 101 It takes encryption 422 using 424 (530). It is CA module 2 about the metadata 1 which includes the information about key Kt' or key Kt' as methods other than this in the transmission line where security was protected. It may transmit to 101 and may save as it is. On the other hand, contents are processed as follows. If all processings about the metadata 414 are completed, enciphered content 409 will be carried out decoding 426 using contents key Kk330 (543), and the contents to which it can view and listen will come to hand.

[0103]Below, the explanatory view about the data flow of after-accumulation viewing and listening is shown in drawing 48 at a removable media. Viewing-and-listening processing of the contents from this HDD4 and same processing are performed also about the viewing-and-listening processing from the ream bubble media 5. However, it is CA module 2 here. After a coincidence check with the metadata 1 accumulated in 101 and the metadata 2 in which the removable media 5 was accumulated, and an conditions-of-contract check are performed, viewing and listening (decoding) of contents is attained. The transmission line where security is protected is used for the encryption metadata 1, and it is personal key Km2. 424 can be inputted in the receiving terminal 3 and can be decoded. The encryption metadata 2 can be decrypted using key Kt' in the decrypted metadata 1. With the contents key Kk stored in the metadata 2, enciphered content is decoded and viewing and listening becomes possible.

[0104]8. Except the receiving terminal which performed the contents viewing viewing-and-listening contract of those other than the receiving terminal which performed the viewing-and-listening contract, the case where it views and listens to contents is shown below. About the relation of movement of the contract contents for viewing and listening, when the candidate for viewing and listening is a contractor, it may be [being those with the move of contract contents, or] nothing, and when the candidate for viewing and listening is the 3rd person, it may be with [of contract contents] a move. Each [about viewing and listening] case is explained below.

[0105](Contractor viewing and listening) The user who performed the viewing-and-listening contract shows first the case where it views and listens to contents. The explanatory view of a point of difference with the primitive operation procedure in the built-in HDD accumulation described in the top is shown in drawing 40.

[0106]** With [of contract contents] a move shows the explanatory view in

contractor viewing and listening to viewing-and-listening-receiving terminal outside drawing 25 by movement of contracted contents. Here, the case where it viewed and listened to contracted contents out of the receiving terminal which performed the viewing-and-listening contract using the card for RMP and the removable media was shown. Like drawing 40 (A), viewing-and-listening contract processing, metadata processing, removable media accumulation, and contents decoding are performed.

[0107]** The explanatory view in contractor viewing and listening is shown without movement of contract contents in viewing-and-listening-receiving terminal outside drawing 26 without movement of contents. here -- the person himself/herself -- by performing the viewing-and-listening contract of contents using receiving terminal RMP1 of possession. The contents themselves are not moved, chisels, such as viewing-and-listening contract information, the contents key Kk, etc. which are accumulated in the card for RMP which performed the viewing-and-listening contract, and the card for RMP, are carried, and the case where it views and listens to the contents in the receiving terminal RMP2 of everything but a movement destination is shown. This service is effective only when the same contents as contract contents are accumulated into the receiving terminal RMP2 of a movement destination. Metadata processing and contents decoding are performed like drawing 40 (B).

[0108]** Gift service can be considered as service to which the 3rd person other than a contractor views and listens to contracted contents out of the 3rd person viewing-and-listening (gift service) receiving terminal. Drawing 28 is a figure usually showing the point of difference between service and gift service. First, a gift contract is explained. A gift refers to that a buyer presents the contents purchased to the receiving terminal which others hold. An IC card cannot be fundamentally owned by individual units, and cannot be transferred to others. Therefore, the system to which a removable media and an IC card can view and listen by a set needs to be a system realized only by being unable to use but transferring a removable media simple substance.

[0109]The explanatory view of the point of difference of a processing object between a contract and a gift contract is usually shown in drawing 41. Under the treaty of a gift, a sender performs viewing-and-listening contract processing, accounting, etc. However, only owner registration processing is delivered without being carried out and considers after a gift contract that the first card for RMP to follow a viewing-and-listening procedure is an owner. An error is returned when the cardholder for RMP concerned does not fulfill the right conditions of contents.

[0110]Below, the lock management and the transmission system of a gift contract are described. The schematic diagram of the information stored in a removable media is shown in drawing 29. The key Kk of enciphered content is entered in metadata. Since gift service is a system realized only in a removable media simple substance, contents and metadata will be stored in the same removable media. Therefore, in order to

protect the key Kk, it is necessary to encipher metadata. Since the key of the encryption metadata cannot be transmitted as it is, a device is required for management and the transmission method of the key Key. Then, a gift key method and a common key system are explained hereafter.

[0111]The information stored in a removable media is shown in drawing 30. First, a gift key method is explained. Or it does not transmit the key of encryption metadata in the case of gift service, the method which transmits only the key information relevant to a key is called a gift key method here. Information required in order to realize gift key methods stored in a removable media, such as key information, is called gift information here.

[0112](1) The explanatory view of the kind of gift key (inherent key) is shown in gift key (inherent key) method drawing 42. In this case, the gift key holds the key with all the common receiving terminals in RMP, and is protected in security. Since the same gift key is stored in all the receiving terminals, acquisition of a key is possible even if it does not transmit the key itself.

** - which does not write down gift key information in only inherent key and removable media common to all the receiving terminal, since it is an only inherent key common to all the receiving terminal, if it can be judged as the contents of a gift contract -- the gift key by the side of a receipt -- decoding of metadata -- possible ** -- common to all the receiving terminal. - which writes down gift key information in the inherent key and removable media of several kinds which can be used arbitrarily, since the key with all same receiving terminal is held, if the key information which can recognize keys, such as key ID, is written down in the removable media -- the gift key by the side of a receipt -- decoding of metadata -- possible ** -- common to all the receiving terminal. - which writes down gift key information in the inherent key and removable media of specification with every service provider, since the key with all same receiving terminal is held, if the key information which can recognize keys, such as key ID, a service provider name, or ID is entered in the removable media, decoding of metadata is possible with the gift key by the side of a receipt -- the required information over the all directions type of these ** - **, For example, in a receiving terminal, it is a gift key, and is gift key information (unnecessary, when using an inherent key common to all the receiving terminal) in a removable media.

[0113](2) Generate a key based on a fixed algorithm one gift key (arbitrary key) method or based on two or more values (initial value). Since the key generation algorithm is the same in all the receiving terminals, if the initial value of a key generation algorithm is transmitted even if it does not transmit the key itself, a key is generable by the receipt side. As required information in this case, in a receiving terminal, it is a key generation algorithm, and is gift key information (initial value) in a removable media, for example.

[0114](3) In the form of **********, using the secret key for every receiving

terminal, and a public key, encipher the key of encryption metadata with a delivery partner's public-key crypto system, and decode the receipt side with your own secret key. The method of accessing a lock management center and getting to know a delivery partner's public key as a method of getting to know a delivery partner's public key, in addition to the method of acquiring information from a delivery partner directly, is also considered. In this case, as required information in a receiving terminal. It is a secret key, a public key, a public key of the address for delivery, and a lock management center access site (required, only when getting to know a delivery partner's public key from a lock management center), and, on the other hand, is a public key (required, only when getting to know a delivery partner's public key from a lock management center) of all the receiving terminals in a center.

[0115](4) -- telling a key delivery center about a common key system delivery partner -- the person himself/herself -- the session key which is a key only for encryption of the key of the encryption metadata is distributed to a possession receiving terminal and a delivery partner possession receiving terminal. The session key distributed from a center is enciphered with the common key system which used the common key of each receiving terminal, or the public key system using the public key of each receiving terminal. The session key distributed from the center is used as a common key, and it is encryption **** of the key of encryption metadata. The receipt side is decoded with a session key. In this case, as required information, they are secret key *1, public key *1, common key *2 with a center, and a lock management center access site in a receiving terminal, for example. a center -- public key *1 of all the receiving terminals, and common key *2 of all the receiving terminals -- it comes out. However, *1 shows a required thing, when enciphering a session key with a public key system, and *2 shows a required thing, when enciphering a session key with a common key system.

[0116](Group contract service) The contents viewing and the accounting object using the card for RMP are individual units fundamentally. However, the service which made group units, such as a family, contents viewing and an accounting object is also considered. First, the feature in HDD accumulation of the contents of a group contract is shown below.

- In the case of entry and viewing and listening, when a group member views and listens to the contents a contract of whose viewing-and-listening contract information written down in the individual profile has been group made [use and] to a whole profile, the viewing-and-listening contract information of group information use and the group contract of a whole profile, Viewing-and-listening contract information is newly written down in the copy of master metadata (default). [0117]Next, the contents which performed the group contract are accumulated in HDD, and procedure (example) in case a group member views and listens to the contents concerned to which the group contract was performed is shown below.

. Depend the S1. televiewer's A IC card A on the insertion S2. televiewer A at PDR. Viewing-and-listening contract S3. master metadata. The group information with which the group member made a contract of a part of metadata from the whole insertion S7. profile to accounting S5. IC card A, and made a contract of the storing S6. televiewer's B IC card B to PDR at a (default) copy and whole profile based on viewing-and-listening contract information entry S4. viewing information, . Required information, including viewing-and-listening contract information etc., comes to hand from storing S8. IC card 1 to IC card 1, and depend required information, including viewing-and-listening contract information etc., on an individual profile's generation S9. televiewer B. check S11. The user who can view and listen views and listens in how from the group information of the whole viewing-and-listening selection S10. profile of contents contracted [viewing-and-listening].[0118]the contents concerned to which the contents which performed the group contract next were accumulated in the removable media, and the group contract was performed for the group member -- the person himself/herself -- the case where it views and listens out of a possession receiving terminal is shown. The changed part of the procedure in the case of removable media accumulation is only change of a storage place. The additional condition and information at the time of a storage place being changed into a removable media from HDD are shown below. That is, there are no conditions in particular of viewing and listening of only the person himself/herself who performed the viewing-and-listening contract. The conditions of viewing and listening of a group member have the following.

- Entry of the group member to which entry of viewing information can view and listen in necessity and a removable media the key with which accumulation of master metadata (default) enciphers the necessity and above-mentioned three information in necessity and a removable media in a key common to all the receiving terminals in a removable media. key information needs to be entered for a removable media -- as required information in this case, for example, in a receiving terminal, it is a key common to a receiving terminal, and they are key information, viewing-and-listening contract information, master metadata (default), and group information in a removable media.

[0119](Viewing-and-listening contract in public environment) As an example to which a viewing-and-listening contract is carried out out of a receiving terminal, the content purchase by the terminal in public environment, such as a KIOSK terminal, occurs. Hereafter, a KIOSK terminal is explained to an example. It is [KIOSK terminal] usable in an unspecified user by inserting a personal IC card (RMP card (CA card 2)). In the KIOSK terminal, the enciphered content which a user can purchase, and the metadata in which the key of enciphered content is entered are stored.

[0120]The process flow of the viewing-and-listening contract in public environment is shown in drawing 27, and the feature is shown in it below.

- Contents and metadata are beforehand distributed to a KIOSK terminal using satellite connection, a land-based line, etc.
- A user inserts an IC card in a KIOSK terminal (S1401).
- It is on the monitor of a KIOSK terminal and search viewing-and-listening contents (S1403).
- Perform the viewing-and-listening contract of selected contents (S1405).
- The media medium containing an IC card and contents can be purchased at the surcharge (S1407) in which a user obtains bringing. When it purchases, an IC card turns into a disposable card for emergencies, and can set up the expiration date.
- A KIOSK terminal transmits a purchase history etc. to a center using a land-based line, and customer relations management and a center control a KIOSK terminal using a land-based line (number-of-sheets management of contents deletion, the IC card for emergencies, and a media medium, etc.). Transmission of accounting information, the payment of a fee, registration of viewing-and-listening contract information, etc. are possible for the KIOSK terminal currently installed in public environment in the center besides the purchase of contents.
- A user views and listens to contents with a receiving terminal, mobile communications equipment, a handheld receiver machine, etc. using an IC card and a media medium (S1409).

[0121]9. Illustrate some of features of conclusion this invention below.

- Media media, such as communication lines, such as a satellite and a land-based line, or a removable media, are used, The time of distributing contents to a home and performing accumulation / copy / reproduction in a home in the digital state, Manage by protecting each rights, such as an owner of a copyright of contents, a broadcasting organization, and a televiewer, for evasion of the situation of infringing on the right of service providers, such as an unjust copy of data which rewrite and exceeds reproduction and private use, a copyright person, or a user, and copyright.
- Set the concept of the copyright protection of contents, and a right protection processing capability to RMP (Rights Management & Protection), and have copyright protection and a right protection function in a receiving terminal.
- The encryption which prevents unjust rewriting and viewing and listening of information for the copyright protection of contents, or the right protection method, A service provider or the user access-restriction right to the contents by a copyright person, Use the electronic watermark etc. which bury information and are crowded in the contents related information (metadata) which stores personal authentication, copyright information, right information data for protection of the contents viewing right by a user, etc. and a digital picture, video, a sound, etc.

[0122]- Use contents, the restricted reception system used as a code of a transmission line as a cipher system of metadata, and the copyright protection cipher system used as a purpose of the copyright protection of contents and metadata, and

right protection.

- In the case of accumulation viewing and listening, accumulate preexisted type broadcast, with the limited reception code at the time of transmission applied, decode a limited reception code at the time of reproduction, accumulate server-based broadcating only in the state of a copyright protection code, and decode a copyright protection code at the time of reproduction, after decoding the limited reception code at the time of transmission.

- Encryption of the contents in the aforementioned copyright protection cipher system and metadata can be enciphered with the transmitting equipment of a service provider, or equipment of a lock management center.

[0123]- Manage the key of the code of the contents in the aforementioned copyright protection cipher system, and metadata in the lock management center.

- In the aforementioned copyright protection cipher system, it is a transmission side, encipher using the contents key Kk in a copyright protection code, and accumulate contents with the key same at a receiver as the same cipher system.

- In the aforementioned copyright protection cipher system, the contents key Kk which is a key to encryption of contents should be stored in metadata, and should be distributed by contents and a set.

- In the aforementioned copyright protection cipher system, if the viewing-and-listening contract of contents finishes, store the contents key Kk in a personal portable CA module.

[0124]- In the aforementioned copyright protection cipher system, only information to be protected should encipher metadata and don't encipher the information without the necessity for protection.

- In the aforementioned copyright protection cipher system, encipher in a copyright protection code at the transmitting side, metadata should be decoded if received by the receiving terminal, and extract required information and the contents key Kk, and be newly re-enciphered with the contents key Kk.

- In order to set the inside of a receiving terminal as personal environment at the time of use, set up personal environment information area, and at the time of receiving terminal use, each user needs to acquire information required for generation of personal environment information area from a personal portable CA module, and needs to generate personal environment information area.

- Information and the contents key Kk required for generation, viewing-and-listening contract information, etc. of personal environment information area should be stored in the personal portable CA module.

[0125]- The accumulation by the user palatability made into the sources of information of the taste information input by a user, or viewing history information as a method of storing up in a mass storage device, There need to be compulsive accumulation etc. which a service provider accumulates in a mass storage medium

compulsorily within the request-to-print-out-files accumulation, emergency and specified time zone by EPG made into sources of information, or the defined capacity about SI, the program information from metadata, etc.

- There are information which should always be stored in a receiving terminal, and information by which portability should be carried out, There are information etc. which are used for the restricted reception system of the group information etc. and the actual condition of having summarized the individual's information as information which should always be stored, It is information required for registration of the content purchase in a KIOSK terminal, and the payment viewing history information on a fee, the contents viewing in other receiving terminals, etc. as information by which portability should be carried out.

- When the same contents as the contents which performed the viewing-and-listening contract by storing viewing history information, the contents key Kk, etc. in a personal portable CA module are accumulated in other receiving terminals, viewing and listening be possible for not performing a viewing-and-listening contract again.

[0126]In a removable media at the time what is called of a gift contract of presenting contents contracted [viewing-and-listening] to the 3rd person, without passing a personal portable CA module - Contents contracted [viewing-and-listening], Store key information, viewing-and-listening contract information, etc., or encipher the key of the metadata which stores the contents key using a common key system or a public key system, and viewing and listening should become possible only using a removable media.

- At the time what is called of a group contract of setting up a viewing-and-listening contract unit and an accounting unit not per individual units but per group, set up the area which summarized all groups' information and sharing of contents contracted [viewing-and-listening] should be attained by the group members in all the members by storing there viewing-and-listening contract information etc.

[0127]

[Effect of the Invention]According to this invention, by using functions, such as encryption, personal authentication, metadata, and an electronic watermark. Right protection of contents can be performed and right protection of contents can be performed by accumulating, after enciphering the metadata and contents in which especially right information data etc. are stored at the transmitting side, processing re-encryption etc. by the receiver and the code's having started HDD. According to this invention, by storing the key to encryption of contents and metadata after a viewing-and-listening contract in a personal portable CA module, also when viewing and listening to contents by other PDR, right protection becomes possible.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The entire configuration figure of the integrated data distribution service about this invention.

[Drawing 2]Comparison of real-time viewing and listening and server type viewing and listening.

[Drawing 3]The explanatory view of the contents enciphered in the transmitting side, and the code gestalt of metadata.

[Drawing 4]Encryption data of BS transmission-line code, and a transmission method of a key.

[Drawing 5]Contents in the case of transmitting the contents key Kk using metadata, a transmission method of metadata.

[Drawing 6]The flow chart which shows the enciphering procedure of the transmitting side.

[Drawing 7]The flow chart which shows the distribution procedure of the transmitting side.

[Drawing 8]The flow chart which shows a receiver procedure.

[Drawing 9]The basic constitution figure of a receiving terminal.

[Drawing 10]The functional block diagram in PDR.

[Drawing 11]The lineblock diagram of cipher processing in RMP.

[Drawing 12]The functional constitution figure in RMP.

[Drawing 13]The primitive operation flow chart from content reception to viewing and listening in a receiving terminal.

[Drawing 14]The explanatory view of the procedure of reception, the cipher system at the time of distribution, and the relation of the code gestalt at the time of accumulation.

[Drawing 15]The figure showing the decoding processing procedure of a transmission-line code.

[Drawing 16]The figure showing an accumulation processing procedure (1/2).

[Drawing 17]The figure showing an accumulation processing procedure (2/2).

[Drawing 18]The figure showing a retrieval processing procedure (1/2).

[Drawing 19]The figure showing a retrieval processing procedure (2/2).

[Drawing 20]The figure showing a viewing-and-listening contract processing procedure.

[Drawing 21]The figure showing an accounting procedure.

[Drawing 22]The figure showing metadata procedure.

[Drawing 23]It is a figure showing a contents decoding procedure (1/2).

[Drawing 24]It is a figure showing a contents decoding procedure (2/2).

[Drawing 25]The explanatory view in contractor viewing and listening by those of contract contents with a move.
[Drawing 26]It is an explanatory view in contractor viewing and listening without movement of contract contents.
[Drawing 27]The process flow of the viewing-and-listening contract in public environment.
[Drawing 28]Usually, the figure showing the point of difference between service and gift service.
[Drawing 29]The schematic diagram of the information stored in a removable media.
[Drawing 30]Information stored in a removable media.
[Drawing 31]A protective method, the purpose, a symbol description figure.
[Drawing 32]The entire configuration figure of the integrated data distribution service about this invention.
[Drawing 33]The explanatory view of required information for a receiving terminal to judge palatability.
[Drawing 34]The explanatory view of the feature of the card for CAS, and the card for RMP.
[Drawing 35]The explanatory view of the information which needs to be made to always fix to PDR.
[Drawing 36]The explanatory view of the information which can carry out portability from PDR.
[Drawing 37]The explanatory view of the main items of a whole profile, and the contents.
[Drawing 38]The explanatory view about the contents of a key table and the retrieving table.
[Drawing 39]Each function of RMP, and the related figure of information area used in that case.
[Drawing 40]The explanatory view of a point of difference with the primitive operation procedure in built-in HDD accumulation.
[Drawing 41]Usually, the explanatory view of the point of difference of a processing object between a contract and a gift contract.
[Drawing 42]The explanatory view of the kind of gift key (inherent key).
[Drawing 43]The explanatory view of the procedure in the contents key transmission system using metadata.
[Drawing 44]The flow chart of the procedure in a contents key transmission system.
[Drawing 45]The flow chart of the contents storage procedure to a removable media.
[Drawing 46]The flow chart of contents viewing procedure.
[Drawing 47]The explanatory view about the data flow of after-accumulation viewing and listening using metadata.
[Drawing 48]It is an explanatory view about the data flow of after-accumulation

viewing and listening to a removable media.

[Description of Notations]

100 ... A receive section, 101 ... A limited reception code descrambler, 102 ... HDD, 103 ... A copyright protection code descrambler, 104 ... Decoder, 110 ... The contents key Kk, 111 ... Kk is embedded at metadata, 112 ... Kw2, 113 ... The scramble key Ks, 120 ... Contents are enciphered by Kk, 121 ... It is Kk to metadata Storing and 122 ... Metadata is enciphered by Kw2, 123 ... They are contents and metadata Encoding and 124 ... TSP is enciphered by Ks, 125 ... Kw2 is enciphered by Kmc and it is distribution and 126 at EMM... Encipher Kw1 by Km1 and it distributes by EMM, 127 ... It is an event Distribution and 128 ... Encipher Ks by Kw1 and it distributes by ECM, 129 ... Kw1 acquisition, 130 ... Ks acquisition, 131 ... Event acquisition, 132 ... Kw2 acquisition, 133 ... Metadata is decoded by Kw2, 134 [... Metadata is read from HDD and it is 138. / ... Metadata is decoded by Kk,] ... It is Kk acquisition and 135 from metadata... It is metadata at Kk Encryption and 136 ... They are contents and metadata HDD accumulation and 137 139 ... It is accumulation and 140 to the card for RMP in a part of metadata... By Kk, contents decoding, 200 ... RMP, 201 ... The card for CAS, 202 ... The card for RMP, 210 ... Reception, 211 ... CAS, 212 ... RMP, 213 ... Accessible HDD, 214 ... Access improper HDD, 215 ... RMP, 250 ... Limited reception code descrambling, 251 ... HDD, 252 ... A copyright protection code descrambler, 300 ... Metadata is decoded by Kw2, 301 ... It is the information on metadata to a retrieving table Storing and 302 ... From metadata to Kk acquisition. 303 ... It is metadata at Kk Encryption and 310 ... Contents information display, 311 ... Reading of metadata, 320 ... An conditions-of-contract display, 321 ... User restriction judgment, 322 ... User request judgment, 330 ... Accounting, 331 ... Viewing-and-listening contract information creation, 340 [... It is metadata decoding and 351 at Kk. / ... Judgment of user restrictions,] ... It is viewing-and-listening contract information to metadata Storing and 341 ... It is storing and 342 to the card for RMP... If required, it is metadata at Km2 Encryption and 350 352 ... It is contents decoding at Kk.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－176419
（P2002－176419A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｂ	５Ｃ０５３
Ｈ０４Ｎ	5/91				６０１Ａ	５Ｃ０６３
	5/92				６０１Ｅ	５Ｃ０６４
	7/08		Ｈ０４Ｎ	5/91	Ｐ	５Ｊ１０４
	7/081			5/92	Ｈ	

審査請求　未請求　請求項の数12　ＯＬ　（全 38 頁）　最終頁に続く

(21)出願番号　特願2000－370936(P2000－370936)

(22)出願日　平成12年12月６日(2000.12.6)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山崎　伊織
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内

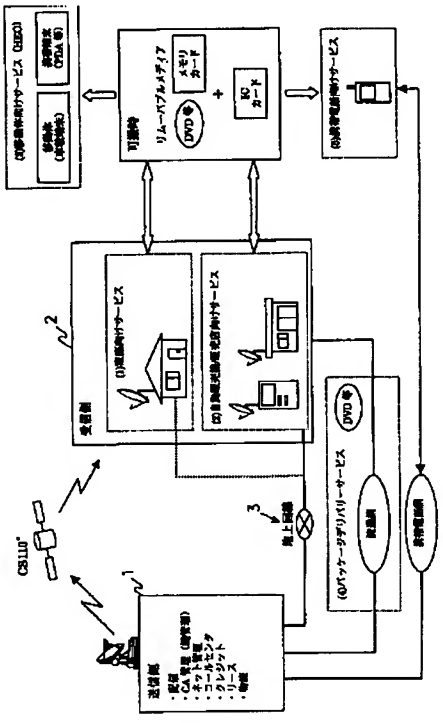
(72)発明者　原田　宏美
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内

(74)代理人　100107010
弁理士　橋爪　健

最終頁に続く

(54)【発明の名称】　権利保護方法

(57)【要約】
【課題】　蓄積媒体に蓄積されているコンテンツの著作権および権利を保護する。
【解決手段】　蓄積媒体内および可搬中のコンテンツの著作権、権利保護を行うために、送信側で、コンテンツを暗号化し、その鍵をメタデータに格納し、メタデータを異なる鍵で暗号化し、暗号化コンテンツと暗号化メタデータセットで配信する。受信端末に受信された暗号化コンテンツと暗号化メタデータは、まず、暗号化メタデータを復号し、コンテンツの鍵を入手し受信端末内のセキュリティが守られた鍵テーブルに保持する。次にメタデータをコンテンツと同じ鍵で再暗号化し、暗号化コンテンツと暗号化メタデータをＨＤＤに蓄積する。視聴コンテンツが選択されたら、メタデータをＨＤＤから読み込み、鍵テーブルから鍵を入手し復号する。その後視聴契約を行い、コンテンツとメタデータの鍵を個人用可搬ＣＡモジュールに格納する。その後、コンテンツの鍵を用いて暗号化コンテンツを復号し、視聴可能となる。



【特許請求の範囲】

【請求項１】受信機内の第１のモジュールに記憶された第２の個人鍵(Km1)を用いて、受信されたスクランブル鍵(Ks)を復号化し、スクランブル鍵(Ks)を用いて暗号化コンテンツ及び暗号化メタデータを含むイベントを生成する限定受信ステップと、
コンテンツとメタデータの権利保護のための著作権保護暗号ステップとを含み、前記著作権保護暗号ステップは、
第２のモジュール又は鍵管理センタに記録された第１の個人鍵(Km2)を用いて、受信された第１の暗号化ワーク鍵(Kw2')を復号化し第１のワーク鍵(Kw2)を生成するステップと、
復号化された第１のワーク鍵(Kw2)を用いて、暗号化メタデータを復号化し、そこに含まれた第１のコンテンツ鍵（Kk）を求めるステップと、
メタデータをコンテンツ鍵（Kk）で暗号化するステップと、
暗号化メタデータ及び暗号化コンテンツを記録媒体に蓄積するステップと、記録媒体から暗号メタデータを読み取り、コンテンツ鍵（Kk）で複号化するステップと、
メタデータの一部を第２のモジュールに蓄積するステップと、
求められた第１のコンテンツ鍵（Kk）を用いて暗号化コンテンツを復号化してコンテンツを生成するステップとを含む権利保護方法。

【請求項２】視聴することが選択された場合、第２のモジュールの情報が視聴条件を満たしているか判断する視聴契約処理と、
メタデータを記録媒体に蓄積するメタデータ処理と、
個人プロファイルの情報を用いて契約済コンテンツを記録媒体から読みこむコンテンツ復号処理とをさらに含む請求項１に記載の権利保護方法。

【請求項３】蓄積することが選択された場合、第２のモジュールの情報が蓄積条件を満たしているか判断する視聴契約処理と、
メタデータをリムーバブルメディアに蓄積するメタデータ処理と、
暗号化コンテンツをリムーバブルメディアに蓄積するリムーバブルメディア蓄積処理と、
第２のモジュールの情報をゲストプロファイルに書き込み、ゲストプロファイルの情報を用いて契約済コンテンツをリムーバブルコンテンツから読みこむコンテンツ復号処理とをさらに含む請求項１又は２に記載の権利保護方法。

【請求項４】メタデータ処理及びコンテンツ復号処理をさらに含み、
メタデータ処理では、
メタデータを第１及び第２メタデータに分離し、
第１メタデータを個人鍵（Km2）で暗号化して第２のモジュールに蓄積し、
第２メタデータを使い捨て鍵（Kt'）で暗号化し、記録媒体に蓄積し、
個人プロファイルの情報を用いて契約済コンテンツを記録媒体から読み込み、コンテンツ復号処理では、
第１及び第２メタデータに従いコンテンツの復号処理を行うことを特徴とする請求項１乃至３のいずれかに記載の権利保護方法。

【請求項５】メタデータ処理及びコンテンツ復号処理をさらに含み、
メタデータ処理では、
メタデータを個人鍵（Km2）で暗号化して第２のモジュールに蓄積し、コンテンツ復号処理では、
第２のモジュールの情報をゲストプロファイルに書き込み、ゲストプロファイルの情報を用いて契約済コンテンツをリムーバブルコンテンツから読みこみ、メタデータとコンテンツに従いコンテンツの復号処理を行うことを特徴とする請求項１乃至３のいずれかに記載の権利保護方法。

【請求項６】前記著作権保護暗号ステップにおけるコンテンツとメタデータの暗号の鍵は鍵管理センタで管理することを特徴とする請求項１乃至５のいずれかに記載の権利保護方法。

【請求項７】前記著作権保護暗号ステップにおいて、メタデータは保護が必要な情報のみ暗号化し、保護の必要のない情報は暗号化しないことを特徴とする請求項１乃至６のいずれかに記載の権利保護方法。

【請求項８】使用時に受信端末内を個人用の環境に設定するために、個人用環境情報エリアを設定しておき、各ユーザーが受信端末使用時に、個人用可搬の第２のモジュールより個人用環境情報エリアの生成に必要な情報を取得し、個人用環境情報エリアを生成することを特徴とする請求項１乃至７のいずれかに記載の権利保護方法。

【請求項９】個人用可搬の第２のモジュール内に個人用環境情報エリアの生成に必要な情報とコンテンツ鍵（Kk）と視聴契約情報が格納されていることを特徴とする請求項１乃至８のいずれかに記載の権利保護方法。

【請求項１０】前記蓄積するステップは、
ユーザーによる嗜好情報入力や視聴履歴情報の情報源としたユーザー嗜好性による蓄積、番組配列情報やメタデータからの番組情報を情報源とした電子番組ガイドによる予約蓄積、又は、緊急時や特定時間帯もしくは定められた容量内でサービスプロバイダが強制的に大容量蓄積媒体に蓄積する強制蓄積のいずれか又は複数の蓄積処理を含むことを特徴とする請求項１乃至９のいずれかに記載の権利保護方法。

【請求項１１】第３者に対して視聴契約済みコンテンツを贈呈するためのギフト契約の時、リムーバブルメディア内に視聴契約済みコンテンツと、鍵情報、又は、共通鍵もしくは公開鍵を用いて暗号化されたメタデータを格

納することにより、リムーバブルメディアのみを用いて視聴可能となることを特徴とする請求項１乃至１０のいずれかに記載の権利保護方法。

【請求項１２】視聴契約単位や課金単位をグループ単位で設定するためのグループ契約の時、グループメンバーの情報を纏めたエリアを設定し、そこに視聴契約情報を格納することにより、グループメンバーで視聴契約済みコンテンツの視聴を可能とすることを特徴とする請求項１乃至１１のいずれかに記載の権利保護方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ配信サービスにおける権利保護方法に関し、特に地上回線や衛星回線を介して配信したデジタルデータをデジタルのまま蓄積して利用するシステムにおいてデータの不正利用を防止する権利保護方法に関する。

【０００２】

【従来の技術】従来のデジタル放送では、サービスチャンネル毎に視聴可／不可の契約を行う契約形態、もしくは同一チャンネル内での時間毎の番組契約を行う契約形態が存在していた。また、既存のデジタル放送等では、各々のコンテンツ単位でのコンテンツの購入を行わせるために、ユーザーがサービス選択後に欲しいコンテンツを選択、契約又は決定し、その契約又は決定と同時にセンタ側との通信を行うようにしている。ユーザーとセンタ側とのリアルタイム通信によって各コンテンツの購入を確認し、確認後契約者に購入許可データを送信することで、ユーザーはコンテンツを購入可能となる。このような双方向リアルタイム購入方式でコンテンツ単位での販売が行われることとなる。

【０００３】暗号化に関しては、今後始まるデジタル放送において、ネットワーク内で使用可能な暗号鍵は数が固定されているため、伝送路で暗号化する／しないの判断がなされる。また、現在の伝送方式では、センタ側で暗号化されたコンテンツは、受信端末内で受信後直に暗号解除を行った後に蓄積装置等に記録される。このように伝送時におけるコンテンツの暗号化は、現在１次暗号のみで行なわれている。

【０００４】

【発明が解決しようとする課題】しかしながら、従来のデジタル放送では、契約時間内での全てのサービス情報を取得することができるが、ユーザーが選択したサービス情報のみの視聴もしくはコンテンツのみの入手は困難である。

【０００５】また、従来のＣＳ／ＢＳなどのデジタル放送でのサービスにおいては、契約形態がチャンネル視聴可／不可、または同一チャンネル内の番組視聴可／不可の契約提供がメインとなっている。これはデジタル放送内における暗号化に用いる鍵の数に制限があるためである。ただし複数の鍵を使用すると鍵の管理が複雑となるだけでなく、複数鍵でのコンテンツの暗号化を行うことで暗号を解くために必要な情報の常時送信となり、現在の伝送量よりさらに多くの情報を伝送しなくてはならない。これは少ない伝送領域においては、困難に近く現実的ではない。また、日々増加するコンテンツ毎に鍵をかけることは、鍵の数が無限大に近くなることであり、これも管理が非常に難しい。さらに、リアルタイム復号に必要な情報を常に伝送しているため、受信端末は、受信時に復号化に必要ＩＣカード等のモジュール（ＣＡ（Conditional Access，限定受信）モジュール）を常時取り付けさせる必要がある。これらのことより、同じチャンネル内の同じ番組の同じ時間において複数の鍵を用いてコンテンツの暗号化を行うことは、困難に近い。

【０００６】また、従来の受信端末では、暗号解除後に再度受信端末内で暗号化を行うことが出来ない。これより受信端末等に存在する蓄積コンテンツを一度復号化した後に、再度暗号化させて蓄積をさせることは不可能であり、また伝送路の暗号化のまま蓄積すると蓄積時における暗号化の鍵扱い等がむずかしくなり、暗号化させて蓄積させるには信頼性等様々な課題が多い。また、デジタル放送を受信する場合において視聴可／不可等の契約を扱う情報が受信端末毎でしか行えないため、受信端末を利用するユーザーが複数の場合、センタ側で複数ユーザー毎の契約形態を認識できない等の課題がある。

【０００７】さらに、例えばコンテンツの第３者に対する譲渡場合等において要求される、著作権保護の方式として電子透かし等のパスワード埋め込みの形式は存在するが、全てのデータ形式に対して有効ではなく、コンテンツのみの保護でしかない。システムとしてコンテンツ並びにコンテンツ関連情報（メタデータ）の両方を保護する方式は現状存在しない。

【０００８】本発明は以上のような課題を解決することを目的とする。例えば、本発明は、暗号化、個人認証、メタデータ、電子すかし等の機能を用いることで、コンテンツの権利保護を行い、特に権利情報等が格納されているメタデータとコンテンツを送信側で暗号化し、受信側で再暗号化等の処理を行いＨＤＤに暗号がかかった状態で蓄積することでコンテンツの権利保護を行うことを目的とする。また、本発明は、視聴契約後にコンテンツとメタデータの暗号化の鍵を個人用可搬ＣＡモジュールに格納することにより、他ＰＤＲでコンテンツを視聴する際にも権利保護を可能とすることを目的とする。

【０００９】また、本発明は、受信端末内で生成した使い捨て鍵を用いてメタデータの作成並びに分割化を行うことで、コンテンツ毎に暗号化可能とする。また、本発明によると、個人を特定できる第２のＣＡモジュールを合わせることで個人特定のサービスを行うようにすることを目的とする。

【００１０】さらに、本発明は、メタデータ内にコンテンツの所有者情報を入れずにおくことで、コンテンツの

譲渡をされた方の受け取り時に初めてコンテンツ所有者が特定できるようにし、ＣＡモジュールへの所有者情報記入が行なわれることにより、第３者への譲渡目的としたコンテンツサービスを実現することを目的とする。

【００１１】

【課題を解決するための手段】本発明は、暗号化コンテンツとそのコンテンツの視聴のために必要なコンテンツ関連情報であるメタデータとによりコンテンツを定義し、また、個人を特定した第２のＣＡモジュールを使用する。これにより、個々に対するサービスの提供を可能とし、また第３者に対する譲渡を目的としたコンテンツの受け渡しにおけるセキュリティ保護も施し、第３者に譲渡を行うサービスの提供を可能とする。

【００１２】ここで、メタデータとは、基本的にコンテンツ以外の情報の総称であり、例えば、コンテンツ制御情報、コンテンツ内容情報、コンテンツ関連情報として定義することができる。概念的には受信端末側でコンテンツを制御するための情報で、例えばコンテンツの蓄積予約を行うための情報（EPG（Electronic Program Guide、電子番組ガイド)に表示するためのコンテンツの名前、ジャンル、配信場所、配信予定日時）、利用制限情報（視聴が可能となるための条件、２０歳以上、男性、○○放送局との契約者）、暗号の鍵等の情報が含まれる。

【００１３】本発明においては、コンテンツ毎の暗号化を行なうために、暗号化コンテンツとそのコンテンツに対する視聴契約形態等の情報を含むコンテンツ関連情報（メタデータ）の分離化を行なう。最初に送信側でコンテンツの暗号化を行ない、暗号化されたコンテンツと同時にメタデータを送信する。この情報を受信した受信側の受信端末では暗号化コンテンツの蓄積、メタデータの伝送路における伝送暗号の復号化および受信端末内で生成される使い捨て鍵による暗号化等の加工を必要に応じて行なった後、送信データの全ての蓄積を行なう。蓄積された暗号化コンテンツを視聴する際は、使い捨て鍵により暗号化されたメタデータを復号化し、有効期限、視聴回数制限、コピー制限、暗号化されたコンテンツを復号するための情報などを埋め込み、再び受信端末内で生成した使い捨て鍵を用いて、メタデータを元にメタデータ１、２の作成並びに分割化を行なう。暗号化コンテンツとメタデータ２をセットとして受信端末の記録媒体等に蓄積し、また残りのメタデータ１をＣＡモジュール等のユーザー個人特定蓄積媒体に書込む。

【００１４】暗号化コンテンツと暗号化メタデータの鍵は、視聴契約後にＣＡモジュールに格納される。ユーザー個人特定蓄積媒体に書込むメタデータは、ユーザー個人の鍵であり、ＣＡモジュール内で暗号化を行なう。ユーザーが契約コンテンツを視聴する際には、検索／課金情報等、受信端末側でこれらの情報を生成したため、受信端末内で視聴契約情報などに基づき再生を行なう。また、暗号化されたコンテンツをセンタ側より送信することで、受信端末内で大容量のコンテンツを暗号化する必要はなく、メタデータのみ暗号化する。これらメタデータ等の情報の解読で復号に必要な情報を入手可能となる。さらにコンテンツ毎に鍵が異なるが、蓄積媒体に蓄積されているコンテンツの鍵の全てが鍵テーブル等に書込まれる。そして、視聴契約済みコンテンツの鍵はＣＡモジュールに格納される。この書込まれた鍵の情報を使用して暗号化コンテンツの再生等を行なうが、再生時のみＣＡモジュール等を必要とするため、常時受信端末に設置する必要はなく、家庭でのコンテンツ購入だけでなく外部などの家庭外への持ち出しでのコンテンツの視聴契約が可能となる。これよりＣＡモジュール等の可搬による受信端末外部での契約も可能となる。よってＣＡモジュール等のユーザー個人特定蓄積媒体は持ち運びが可能となる。また、受信端末で蓄積した暗号化コンテンツはユーザーの視聴時に暗号化されたコンテンツを複写し、同様に暗号化されたメタデータも複写し、複写したメタデータを復号化したのち復号化したメタデータを使用することにより複写されたコンテンツを復号化して再生する。これより暗号化されたコンテンツデータは常時蓄積された状態となり、いつでも別のＣＡモジュールで同様のサービスを享受することが可能である。さらに、本発明では、ＣＡモジュールを受信機内に装着するものと、可搬可能なものの複数に分けるようにしている。

【００１５】

【発明の実施の形態】以下の見出しに従い説明する。

１．権利の保護の概要
２．著作権保護方式
３．暗号システム
４．受信端末
５．ＲＭＰ
６．受信端末（ＰＤＲ）で使用される情報
７．受信端末（ＰＤＲ）アプリケーション
８．視聴契約をおこなった受信端末以外におけるコンテンツ視聴

【００１６】１．権利の保護の概要

（サービス概要）本発明で示す、総合データ配信サービスは、衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いて、家庭にコンテンツを配信し、家庭内でデジタルのまま蓄積／コピー再生を行うことを目的としている。これに伴い、データの不正な書き換え、再生、私的利用を超えるコピー等のサービスプロバイダ、著作権所有者もしくはユーザーの権利、著作権を侵害する事態が起こりかねない。そのためコンテンツの著作権者、放送事業者、視聴者など各々の権利を保護、管理する必要がある。本発明では、例としてデジタル衛星放送を用いたデータ配信を想定して説明する。

【００１７】（権利保護）コンテンツの著作権保護もし

くは権利保護方法には、例えば以下のようなものがある。
（１）情報の不正な書き換えおよび視聴を防ぐ暗号化、（２）サービスプロバイダもしくは著作権所有者によるコンテンツへのユーザーアクセス制限権利と、ユーザーによるコンテンツ視聴権利の保護のための個人認証、（３）著作権情報もしくは権利情報等の格納フォーマットであるメタデータ、（４）デジタルの画像、ビデオ、音声等の中に情報をうめこむ電子すかし。
【００１８】図３１に、保護方法と目的、機能の説明図を示す。ここでは概要を説明することとして、詳細は後述する（２．著作権保護方式参照）。暗号化の目的には、情報の不正な書き換え防止や情報の不正な視聴防止等があり、その機能としてコンテンツやメタデータの暗号化等が想定される。個人認証の目的には、第１に、サービスプロバイダ、著作権所有者のコンテンツへのユーザーアクセス制限権利の保護があり、その機能として、著作権情報、権利情報のユーザーアクセス制限と個人情報との照らし合わせが想定される。また、個人認証の目的には、第２に、ユーザーのコンテンツ視聴権利の保護があり、その機能として、個人単位の契約情報に沿ったコンテンツにアクセスが想定される。さらに、第３にプライバシーの保護があり、その機能として、本人のみ個人情報にアクセス可能が想定される。その他にも、個人を判別する時など個人に関係する際等に、様々な目的で用いられる。メタデータの目的には、著作権情報、権利情報の使用等があり、その機能として、コンテンツとセットで用い、そのコンテンツの著作権情報、権利情報を格納等が想定される。電子すかしの目的にはコンテンツに対する不正使用の抑止等があり、その機能として、コンテンツの不正使用時にアプリケーションより使用不可が可能等が想定される。
【００１９】（システム概要）図１に、本発明に関する総合データ配信サービスの全体構成図を示す。また、図３２に、全体システム構成の補足説明図を示す。全体システムは、コンテンツの制作、配信等を行う送信側１と受信端末等から構成される受信側２に大きく分けられる。
【００２０】送信側１は、送信センタ、鍵管理センタ、地上回線管理センタ、顧客管理センタ、物流管理センタ等を備える。送信側１の主な特徴として、コンテンツおよび関連情報の制作、配信や、著作権、権利等を考慮したコンテンツの暗号化、鍵管理および、視聴履歴等の情報の収集、管理等があげられる。
【００２１】受信側２は、受信端末、KIOSK端末、販売店、その他に拡張として、移動体、携帯電話等を備える。受信端末の主な特徴として、コンテンツおよび関連情報を蓄積するための、大容量蓄積媒体の装備と、暗号化コンテンツ、関連情報の複合および関連情報の再暗号化と、個人単位の認証および課金が可能等があげられる。KIOSK端末は、店、コンビニエンスストア、公共施設等に設定される情報案内・サービスのための端末である。その主な特徴を、送信側から受信側と、受信側から送信側のアクションに分けて示すと、まず、送信側から受信側のアクションの特徴として、例えば衛星回線もしくは地上回線を用いて、コンテンツおよび関連情報の配信と、暗号化コンテンツ、関連情報の鍵もしくは鍵情報の配信があげられる。また、受信側から送信側のアクションの特徴として、地上回線を用いて課金処理情報の送信と、視聴履歴、リクエスト等の個人情報の送信等があげられる。
【００２２】伝送路３は、衛星、地上回線、流通網、その他に拡張として携帯電話網等から構成される。地上回線の主な特徴を、送信側から受信側と、受信側から送信側のアクションに分けて示す。送信側から受信側のアクションの特徴として、コンテンツおよび関連情報の配信と、暗号化コンテンツ、関連情報の鍵もしくは鍵情報の配信等があげられる。受信側から送信側のアクションの特徴として、地上回線を用いて、課金処理情報の送信と、地上回線を用いて視聴履歴、リクエスト等の個人情報の送信があげられる。
【００２３】（全体システムにおける処理）本発明で示す総合データ配信サービスにおける、全体システムの基本的な暗号システムについて以下に示す。まず、送出側のサービスプロバイダの編集システムにおいてコンテンツとメタデータの制作、編集を行い、鍵管理センタにコンテンツとメタデータを専用回線等を用いて伝送する。鍵管理センタは、コンテンツに対して、著作権を保護するためにかける暗号（著作権保護暗号）をかけ、その鍵の管理を行い、暗号化コンテンツと必要であればその鍵をサービスプロバイダに伝送する。暗号化コンテンツの鍵は、地上回線や衛星回線等を用いて受信端末に送信する事も考えられる。メタデータも同様な処理を施される。コンテンツとメタデータの暗号化はサービスプロバイダで行われる事もある。その後、コンテンツとメタデータの伝送形態である例えばMPEG-2 TSに暗号（限定受信暗号）をかけ、配信する。配信されたデータは受信側の受信端末で受信され、受信端末内で限定受信暗号の復号を行う。その後、コンテンツとメタデータを著作権保護暗号がかかったまま大容量蓄積媒体（例として以降ＨＤＤとして説明する）に蓄積し、視聴の際に復号する。
【００２４】（視聴）コンテンツ等の視聴に関しては、例えば、リアルタイム視聴と蓄積型視聴がある。リアルタイム視聴とは、サービスプロバイダから配信されるコンテンツをリアルタイムで視聴する事を示す。リアルタイム視聴サービスとして、大容量蓄積媒体を持たない受信端末を想定したリアルタイム視聴のみを対象とした既存型放送と、大容量蓄積媒体を持つ受信端末を想定した蓄積サービスとリアルタイムサービスを対象としたサーバー型放送が想定される。既存型放送の暗号方式は限定

受信暗号のみを用い、サーバー型放送の暗号方式は限定受信暗号と著作権保護暗号を用いる。蓄積型視聴とは、サービスプロバイダから配信されるコンテンツを大容量蓄積媒体に蓄積後に視聴する事を指す。

【００２５】既存型放送とサーバー型放送を蓄積する場合の暗号形態について以下に示す。既存型放送は、伝送時の限定受信暗号をかけたまま蓄積し、再生時に限定受信暗号デスクランブラにより復号する形態とする。ただし、伝送時の暗号方式のみであるため一部サービス（個人契約等）に制限が生じる場合がある。サーバー型放送は、伝送時の限定受信暗号を復号後、著作権保護暗号のみの状態で蓄積し、再生時は著作権保護暗号デスクランブラにより復号する形態とする。

【００２６】（リアルタイム、蓄積視聴比較）図２に、リアルタイム視聴とサーバー型視聴の比較を示す。この図は、既存型放送とサーバー型放送における、リアルタイム視聴と蓄積視聴の際の受信端末内処理手順を示している。このシステムは、受信部１００、ＨＤＤ１０２以外に、限定受信暗号デスクランブラ１０１と著作権保護暗号デスクランブラ１０３とデコーダ１０４を含む機能をＲＭＰ（Rights Management & Protection）１０５として備え、コンテンツの著作権、権利保護処理機能を示している。

【００２７】既存型放送のリアルタイム視聴の暗号処理手順では（点線参照）、受信機（ＰＤＲ）に受信されたコンテンツは、受信部１００を通り、限定受信暗号デスクランブラ１０１で復号された後、デコーダ１０４を通り視聴可能となる。既存型放送の蓄積視聴の暗号処理手順では（破線参照）、受信端末に受信されたコンテンツは、受信部１００を通り、限定受信暗号デスクランブラ１０１を通らずにＨＤＤ１０２に蓄積される。視聴の際、ＨＤＤ１０２から読み出され限定受信暗号デスクランブラ１０１で復号され、デコーダ１０４を通り視聴可能となる。サーバー型放送のリアルタイム視聴では（実線参照）、ＰＤＲに受信されたコンテンツは、受信部１００を通り、限定受信暗号デスクランブラ１０１で復号される。その後、著作権保護暗号デスクランブラ１０３で復号された後、デコーダ１０４を通り視聴可能となる。サーバー型放送の蓄積視聴では（２点鎖線参照）、ＰＤＲに受信されたコンテンツは、受信部１００を通り、限定受信暗号デスクランブラ１０１で復号されＨＤＤ１０２に蓄積される。その後、視聴の際にＨＤＤ１０２から読み出され、著作権保護暗号デスクランブラ１０３で復号された後、デコーダ１０４を通り視聴となる。

【００２８】（蓄積）以下にＨＤＤへの各種の蓄積について説明する。

（１）ユーザー嗜好性による蓄積

本発明で示す、総合データ配信サービスの特徴の１つとして、有限な蓄積媒体を効率的に管理させる蓄積エージェント機能を有する。本サービスにおける蓄積エージェント機能とは、配信されるコンテンツから、ユーザーの嗜好にそったコンテンツを自動的にＨＤＤ内に蓄積するものである。ＨＤＤの容量が許す限り、配信する全てのコンテンツを蓄積する事も可能である。

【００２９】本チャンネルに契約しているユーザーは、本チャンネル全てのコンテンツを受信端末で受信可能である。受信されたコンテンツは、ユーザー嗜好に基づいて自動的に選定され、ＨＤＤ内に蓄積される。ユーザーはＨＤＤ内のコンテンツより、キーワード検索、ジャンル検索等を行い、視聴を望むコンテンツを選択し、視聴する。このシステムは、自動的に選択・蓄積されたコンテンツの中から、ユーザーが選択したコンテンツにのみ課金される仕組みになっている。

【００３０】図３３に、受信端末が嗜好性を判断するための必要な情報の説明図を示す。処理形態として、受信端末の能動的処理と自律的処理がある。能動的処理では、ユーザーが受信端末に情報(ジャンル、キーワード、職業、趣味等)を入力する(ユーザーの意思有り)。一方、自律的処理では、ユーザー情報(視聴履歴、検索履歴、個人情報等)を用いる(ユーザーの意思無し)。

【００３１】（２）ＥＰＧによる蓄積

EPG（Electronic Program Guide）とは、電子番組ガイドのことである。EPGは、放送局が送出するSI情報を利用して、受信機側で番組情報を構成し番組選択の手段とするものである。SI（Service Information）とは、番組配列情報のことである。SIは、番組選択の利便性のために規定された各種情報である。SIはまた、郵政省令で定義され、内容はARIB規格として規定される。さらに、SIは、ARIB規格独自の拡張部分に加えて、MPEG-2のPSI情報も含まれる。主に、番組表表示、番組検索、番組予約の用途に用いられる。番組表表示、番組検索等の作業を行った後、番組の予約（ＨＤＤへ予約録画）が考えられる。EPGで表示させる情報として、番組タイトル、番組サブタイトル、放送時間、放送事業体名、有料/無料、パレンタルの有無、デジタルコピー可否等の情報が表示されると考えられる。EPGを作成する情報源として、SIとメタデータが想定される。

【００３２】（３）強制蓄積

視聴者の要求による蓄積ではなく、緊急放送、お知らせ等のコンテンツを送信側より強制的に蓄積させる機能である。受信端末がコンテンツ受信可能状態（電源、アンテナ等）であれば、緊急時に視聴者の許諾なしにコンテンツの蓄積が行われる機能である、強制書き込みと、事前に視聴者とサービス提供者との間で蓄積媒体内の使用可能容量を取り決め、その容量の範囲であればサービス提供者が、視聴者の許諾なしに定期的にコンテンツの蓄積を行える機能である定期的書き込みと、サービス提供者の制御のもとで、受信端末に対してコンテンツの蓄積時間を指定し、指定された時間により受信端末がコンテンツを蓄積する機能である時間帯指定書き込み等が考え

られる。

【００３３】２．著作権保護方式

図３１に示した暗号化、個人認証、メタデータによる各保護方法について以下に詳述する。

（暗号化、ＲＭＰ）データの不正な書き換え、再生、私的利用を超えるコピー等の権利、著作権を侵害する行為を回避するためには、視聴制御、蓄積制御、コピー制御等の処理が必要となる。これらの、コンテンツの著作権、権利保護処理を行う機能を、ＲＭＰ（Rights Management & Protection）とする。ＲＭＰに関連する、コンテンツを不正な書き換えおよび視聴から保護する暗号化や個人単位のコンテンツへのアクセス制御を行う個人認証さらに著作権、権利情報が記述されているメタデータの各項目について以下に示す。

【００３４】まず、コンテンツ暗号化方式について説明する。コンテンツの不正な視聴、コピーおよび書き換えから回避するためには、コンテンツの暗号化は必須である。本発明で示す総合データ配信サービスは、受信端末内のＨＤＤに蓄積するサービスを想定しているので、ＨＤＤ内のコンテンツ保護を考慮する必要があり、コンテンツに暗号をかける必要がある。本総合データ配信サービスにおいて用いられる暗号方式は著作権保護暗号方式と限定受信方式である。著作権保護暗号方式は、本総合データ配信サービス特有の暗号方式であり、コンテンツ自体を暗号化する。限定受信方式は、ＢＳデジタル放送における限定受信方式であり、暗号方式は、一例として、Multi２を用いる。

【００３５】著作権保護暗号方式の特徴を以下に示す。著作権保護暗号方式は、配信用データの組み立て後ではなく、コンテンツの制作完了時にコンテンツのデータ自体を暗号化し、ファイルフォーマットの区別なく暗号化が可能である。暗号化単位はコンテンツ単位となり、最小暗号化単位はリソースおよびストリームである。そして、暗号化単位ごとに異なる鍵を用いることが可能である。

【００３６】つぎに、メタデータ暗号化方式について説明する。本発明で示す総合データ配信サービスでは、コンテンツとセットでメタデータを配信する。メタデータにはコンテンツの検索情報の他に、著作権、権利保護の為に必要な情報が記述されている。よって、コンテンツの著作権、権利保護のためには、コンテンツの暗号化と同時に、メタデータの暗号化も必要である。その際、必ずしもメタデータ全てを暗号化する必要はなく、保護が必要な情報（著作権、権利情報）等のみ暗号化処理を行い、保護の必要のない情報は暗号化処理を行わないシステムも考えられる。

【００３７】（個人認証）個人認証の手段として、ＣＡモジュールと個人プロファイルが考えられる。ＣＡモジュールを個人用とし、各個人が携帯することにより、ユーザーとＣＡモジュールの認証手段とし、ＰＤＲ内に個人プロファイルを設定する事により、ＣＡモジュールとＰＤＲの認証を行う事が可能となる。

【００３８】まず、ＣＡモジュールについて説明する。個人認証を実現させる手段として、ＣＡモジュールを用いる。従来（BS/CSデジタル放送）のＣＡモジュールは、受信端末に対して1枚であり固定である。そして、家族、グループ単位による視聴契約、課金契約となる。受信端末に対して、1枚のＣＡモジュールでは、受信端末単位の視聴契約、課金処理となる。そこで、本発明で示す総合データ配信サービスではＣＡモジュールを2種類（ＣＡＳ用カード、ＲＭＰ用カード）用意して、個人認証をさせ、個人単位の視聴契約および課金処理を行う。具体的な実現手段としては、ＣＡＳ用カードには、従来のＣＡモジュールと同じ機能であるコンテンツの受信に関係する機能を持たせ、ＲＭＰ用カードは蓄積コンテンツへのアクセス、視聴契約および課金処理等に関係する機能を持たせる。

【００３９】さらに、ＲＭＰ用カードには可搬性を持たせることで、個人単位で携帯可能とする。この事より、個人単位の視聴契約、課金処理等が可能となる。ＣＡモジュールとしては、ICカードやスマートメディア等が考えられる。これ以降は、例としてＣＡモジュールをICカードとして説明する。ＣＡモジュールにクレジット機能等の付加機能を付ける事によりe-commerce等の新サービスへ拡張が可能である。

【００４０】図３４に、ＣＡＳ用カード、ＲＭＰ用カードの特徴の説明図を示す。ＣＡＳ用カードは、受信端末内に常時設備されていて、通常、受信端末単位で一枚用いられる。よって、視聴権利単位、課金単位は、家族もしくはグループ単位となる。使用目的は限定受信方式であり、課金対象物はサービス、イベントである。よって、視聴契約方法は事前契約となる。一方、ＲＭＰ用カードは、可搬性を持ち、個人単位で配布され、個人が携帯することができる。よって、視聴権利単位、課金単位は、個人単位となる。しかし、グループ単位で事前に契約を行っている時はグループ単位が視聴権利単位、課金単位となる。使用目的はＲＭＰ全体における使用であり、課金対象物はコンテンツである。その際の視聴契約方法は視聴契約を行う事で視聴可能となる方法を用いる。

【００４１】つぎに、個人プロファイルについて説明する。受信端末は、複数のユーザーが使用する。受信端末では、個人単位での視聴契約、課金処理等が行われるので、受信端末を使用するたびに、使用ユーザー用に使用環境を変更する必要がある。環境を設定するための情報を、ＲＭＰカードから入手して、ＰＤＲを使用している間格納しておくエリアを個人プロファイルと呼ぶ。個人の使用環境に基づいた、主な処理として、事前契約チャンネルの判断、ユーザーが視聴可能なコンテンツかの判断（年齢、性別等の条件等）、視聴契約処理、課金処

理、視聴処理等が考えられる。これらの処理に用いられる情報は、ＲＭＰ用カードおよび個人プロファイルのいずれかから入手する。

【００４２】ＲＭＰ用カードを挿入すると、個人プロファイルが立ち上がり、個人プロファイルの生成に必要な情報をＲＭＰ用カードから入手する。その個人プロファイルの情報をもとに、受信端末内の環境がＲＭＰ用カード所有者用の環境となる。ＲＭＰカードを外すと、ＲＭＰ用カードから入手した情報は個人プロファイルから消去される。受信端末所有者でないユーザーが、受信端末を使用する場合は、ゲストユーザー用のプロファイルである、ゲストプロファイルが立ちあがり、個人プロファイルと同様にＲＭＰ用カードから必要な情報を入手し、ゲストプロファイルに書き込む。ＲＭＰ用カードを外すとゲストプロファイルに記入されている情報は消去される。個人プロファイルとゲストプロファイルは同じエリアを利用することも可能である。よって、ＲＭＰ用カードには個人プロファイル生成に必要な情報が記入されている必要がある。

【００４３】（メタデータ）まず、メタデータに格納される情報には、大きく分けると権利メタデータと検索メタデータが存在する。本発明で示す総合データ配信サービスでは、メタデータには検索、課金、コンテンツの鍵情報、著作権情報等が含まれる。権利メタデータ、検索メタデータについて以下に示す。

【００４４】まず、権利メタデータについて説明する。権利メタデータは、著作権や権利に関わる情報が記述してあるメタデータである。著作権保護には当該情報を用いる。権利メタデータの主な項目を以下に示す。

【００４５】（１）　暗号化方式に関する情報

暗号の有無、使用している暗号化方式、鍵の情報等を含む情報であり、一部暗号化される情報である。ＲＭＰ内で暗号化方式、鍵情報等、情報が書き換えられる場合がある。主な項目を以下に示す。

・コンテンツの暗号方式
・メタデータの暗号方式
・暗号の有無
・鍵、もしくは鍵情報

【００４６】（２）　権利に関する情報

コンテンツの著作権に関する情報を含む情報であり、放送時に固定され全て暗号化される情報である。主な項目を以下に示す。

・権利者
・権利種別
・管理先

【００４７】（３）　契約情報（許諾情報）

視聴契約時に画面に提示すべき利用条件等を含む情報であり、放送時に固定され、全て暗号化される情報である。主な項目を以下に示す。

・コピー許可
・蓄積許可
・年齢制限
・有効期限
・料金

【００４８】（４）　課金情報

課金処理時に必要となる情報を含む情報であり、視聴契約時に一部情報が書き込まれ全て暗号化される情報である。主な項目を以下に示す。

・課金方法
・課金処理状態

【００４９】（５）　個人認証情報

視聴契約時、蓄積時等の個人認証が必要な時に利用される情報であり、ＲＭＰ内でＲＭＰ用カード、プロファイルから情報が書き込まれ、一部暗号化される情報である。主な項目を以下に示す。

・利用者の個人ID
・年齢
・性別

【００５０】（６）　利用状況に関する情報

蓄積、コピーされたコンテンツに対する保護を行なう際に必要となる情報であり、ユーザーの利用により毎回書き換わる情報で、データ改ざん、不正使用から守るため全て暗号化される。主な項目を以下に示す。

・累積利用時間
・利用回数
・視聴日時

【００５１】（７）　蓄積に関する情報

コンテンツ、メタデータを蓄積する際に必要となる情報であり、一部蓄積時等に書き換えられる。主な項目を以下に示す。

・蓄積場所の指定
・蓄積方法

【００５２】つぎに、検索メタデータについて説明する。検索メタデータは、検索に関わる情報が記述してあるメタデータである。検索処理には当該情報を用いる。しかし、検索エンジンによっては、権利メタデータの情報を検索情報として使用する可能性もある。検索メタデータの主な項目を以下に示す。

【００５３】（１）　コンテンツ自体の属性情報

他のコンテンツ、メタデータと区別するための情報であり、放送時に固定される情報である。主な項目を以下に示す。

・コンテンツID
・コンテンツ名
・有料の有無

【００５４】（２）　番組/サービスの属性情報

番組/サービスを表現する情報であり、検索テーブルに格納する情報を含む。放送時に固定される情報である。主な項目を以下に示す。

・番組名

・チャンネル名
・キーワード
・概要
・放送事業者コード
【００５５】３．暗号システム
（暗号方式）本発明で示す総合データ配信サービスの暗号方式には著作権保護暗号方式と限定受信方式がある。図３に、送信側において暗号化されたコンテンツ、メタデータの暗号形態の説明図を示す。まず、コンテンツ、メタデータの制作終了の時点で、コンテンツをファイルもしくはストリーム単位で著作権保護暗号で鍵Kk　１１０を用いて暗号化する。その鍵をメタデータに埋め込み１１１メタデータファイルを著作権保護暗号で鍵Kw2　１１２を用いて暗号化する。それら暗号化コンテンツ、暗号化メタデータの伝送形態であるMPEG-２ TSを鍵Ks　１１３で暗号化する。
【００５６】（鍵配信方式）まず、映像ストリームの伝送について説明する。一般に、映像ストリームは、固定長のデータにブロック化される。各ブロックにはヘッダ情報が追加される。TSP（Transport Stream Packet）は、このヘッダとデータの組であり、伝送時のデータパケットのフォーマットを指す。既存型でスクランブル（暗号）を掛ける場合はデータ部分を暗号化する。ECM（Entitlement Control Message）は、ユーザー全体に共通的に伝送される情報であり、番組情報および制御情報を含む共通情報の伝送メッセージである。番組情報とは、例えば、番組に関する情報とデスクランブルのための鍵などであり、制御情報とは、例えば、デコーダのデスクランブル機能の強制オン／オフの指令などである。ECMは、基本的にコンテンツのスクランブル鍵を伝送するため、コンテンツと共に伝送されるものであり、ある特定ユーザーに限定して送られる情報ではない。また、EMM（Entitlement Management Message）は、加入者毎の契約情報および共通情報の暗号を解くためのワーク鍵を含む個別情報の伝送メッセージである。EMMは、基本的にユーザーが契約した事業者の鍵等を送るため、ある特定ユーザーを限定して送られる情報である。また、ＣＡ（Conditional Access）systemとは、限定受信方式を指し、サービス（編成チャンネル）やイベント（番組）の視聴を暗号化鍵で制御するシステムである。以下に、限定受信方式と著作権保護暗号方式の、暗号化データ及び鍵の配信方法を示す。
【００５７】（限定受信方式）図４に、BS伝送路暗号の暗号化データ及び鍵の伝送方法を示す。まず、コンテンツ、メタデータ等を含んだイベントの伝送形態であるTSパケットに対して、スクランブル鍵Ksで暗号化する。次にスクランブル鍵Ksをワーク鍵Kw1で暗号化し、鍵Ks'を作成する。この時のワーク鍵Kw1は放送サイドの事業者毎に定めている鍵であって、本サービスの視聴可、不可に関わる鍵である。最後に、ワーク鍵Kw1を各受信端末毎に一意である個人鍵Km1で暗号化し、鍵Kw1'を作成する。これら、暗号化されたデータ及び鍵を、暗号化イベントデータはBS伝送路、鍵Ks'はECM、鍵Kw1'はEMMを用いて伝送する。それら暗号化データを受信した受信端末はＣＡモジュール1内に格納されている個人鍵Km1を用いて復号する。まず、EMMで伝送された鍵Kw1'を個人鍵Km1を用いて復号し、ワーク鍵Kw1を入手する。次に、ECMを用いて伝送されたKs'をワーク鍵Kw1を用いて復号し、スクランブル鍵Ksを入手する。最後に、BS伝送路を用いて伝送された暗号化イベントデータをスクランブル鍵Ksを用いて復号し、イベントの伝送形態であるTSパケットを入手する。
【００５８】（著作権保護暗号方式）図５に、コンテンツ鍵Kkをメタデータを用いて伝送する場合のコンテンツ、メタデータの伝送方法を示す。まず、コンテンツをコンテンツ鍵Kkで暗号化する。コンテンツ鍵Kkは各コンテンツごとに異なる鍵を用いる事が可能である。しかし、各サービスプロバイダや等のある集合で共通であったり、全て共通であることも可能である。そのコンテンツ鍵Kkをメタデータに追記し、メタデータをワーク鍵Kw2で暗号化する。この時のワーク鍵Kw2は各サービスプロバイダ等のある集合毎に異なる鍵を用いたり、全て共通である事も可能である。そして、BS伝送路暗号で用いられる鍵Kw1を用いる事も可能である。最後に、ワーク鍵Kw2を各受信端末毎に一意もしくは全て共通である鍵Kmcで暗号化し、鍵Kw2'を作成する。これら、暗号化されたデータ及び鍵を、暗号化コンテンツと暗号化メタデータはBS伝送路を用いて伝送し、鍵Kw2'はEMMを用いて伝送する。それら暗号化データを受信した受信端末は受信端末内に格納されている鍵Kmcを用いて復号する。まず、EMMで伝送された鍵Kw2'を鍵Kmcを用いて復号し、ワーク鍵Kw2を入手する。次に、BS伝送路を用いて伝送された暗号化メタデータをワーク鍵Kw2を用いて復号し、メタデータを入手する。最後に、BS伝送路を用いて伝送された暗号化コンテンツをメタデータに記入されているコンテンツ鍵Kkを用いて復号し、コンテンツを入手する。
【００５９】（暗号処理手順）本サービスにおける暗号処理の概要を以下に示す。蓄積媒体内および可搬中のコンテンツの著作権、権利保護を行うために、送信側で、コンテンツを暗号化し、その鍵をメタデータに格納し、メタデータを異なる鍵で暗号化し、暗号化コンテンツと暗号化メタデータセットで配信する。受信端末に受信された暗号化コンテンツと暗号化メタデータは、まず、暗号化メタデータを復号し、コンテンツの鍵Kkを入手し受信端末内のセキュリティが守られた鍵テーブルに保持する。次にメタデータをコンテンツと同じ鍵で再暗号化し、暗号化コンテンツと暗号化メタデータをＨＤＤに蓄積する。視聴コンテンツが選択されたら、メタデータをＨＤＤから読み込み、鍵テーブルから鍵を入手し復号する。その後視聴契約を行い、コンテンツとメタデータの

鍵を個人用可搬ＣＡモジュールに格納する。鍵を個人用ＣＡモジュールに格納することにより、他受信端末でもコンテンツの視聴が可能となる。全ての処理が終わった後、コンテンツの鍵を用いて暗号化コンテンツを復号し、視聴可能となる。

【００６０】全体システムにおける暗号処理手順をフローチャートを用いて具体的に以下に示す。それぞれ、図６は送信側の暗号化手順で、図７は送信側の配信手順で、図８は受信側手順を示すフローチャートである。

【００６１】まず、図６の送信側の暗号化手順について示す。はじめに著作権保護暗号をかける。まず、コンテンツを構成しているファイル、ストリームをファイル単位もしくはストリーム単位で鍵Kkにより暗号化する（１２０）。この際、コンテンツ単位内のファイルは同一の鍵Kkを使用する。そして、暗号化コンテンツの鍵Kkをメタデータに格納し（１２１）、メタデータを鍵Kw2で暗号化する（１２２）。次に限定受信暗号をかける。コンテンツ、メタデータを伝送フォーマットであるMPEG-2 TSにエンコードし（１２３）、TSパケット（TSP）のペイロードを鍵Ksで暗号化する（１２４）。

【００６２】次に図７の送信側の配信手順について示す。事前にワーク鍵Kw2を鍵Kmcで暗号化し、鍵Kw2'としてEMMを用いて配信する（１２５）。同様に、ワーク鍵Kw1を個人鍵Km1で暗号化し、鍵Kw1'としてEMMを用いて事前に個別配信する（１２６）。その後、放送時間に鍵Ksで暗号化されたイベントを配信する（１２７）。そして、鍵Ksをワーク鍵Kw1で暗号化し、ECMを用いて配信する（１２８）。

【００６３】次に図８の受信側手順について示す。はじめに限定受信方式の処理を行う。ＣＡＳ用カード（ＣＡモジュール１）内の個人鍵Km1を用いて、暗号化された鍵Kw1を復号し、鍵Kw1を入手する（１２９）。そして、暗号化Ksを鍵Kw1で復号し、鍵Ksを入手する（１３０）。暗号化イベントを鍵Ksで復号し、イベントを入手する（１３１）。次に著作権保護暗号方式の処理を行う。まず、事前にＰＤＲ内にデフォルトで格納されている個人鍵Kmcを用いて、暗号化されたKw2を復号し、鍵Kw2を入手する（１３２）。個人鍵KmcはデフォルトでＲＭＰ用カード（ＣＡモジュール2）内に用意されている鍵であるが、鍵管理センタ等により更新する事も可能である。次に暗号化メタデータを鍵Kw2で復号し（１３３）、鍵Kkを入手する（１３４）。そして、メタデータを鍵Kkで暗号化し（１３５）、ＨＤＤに蓄積する（１３６）。また、暗号化コンテンツは、そのままＨＤＤに蓄積される。なお、鍵Kkは受信機内のセキュリティーが守られた鍵テーブルに保持する。その後、ユーザーが視聴を望むコンテンツを選択したら、暗号化メタデータをＨＤＤから読み出し（１３７）、鍵テーブルに保持されていた鍵Kkを用いて復号する（１３８）。視聴契約後、視聴契約情報を記入し、メタデータの一部（視聴契約情報、鍵Kk等）をＲＭＰ用カードと必要であれば全体プロファイルに格納する（１３９）。視聴契約情報とは、契約コンテンツID、契約日時、契約条件、課金情報等コンテンツの視聴や契約および課金に関わる情報である。視聴契約およびメタデータに関わる処理が終わったら、暗号化コンテンツをＨＤＤから読み出して、鍵Kkを用いて復号する（１４０）。

【００６４】ここで、コンテンツの暗号処理における主な特徴を以下に示す。第１に送信側で著作権保護暗号方式を用いて、鍵Kkで暗号化されて配信される。第２に送信側でかけた暗号方式と同じ暗号方式である著作権保護暗号がかかったまま、ＨＤＤに蓄積される。すなわち、暗号化コンテンツは鍵Kkで暗号化されたままである。第３に視聴契約が終わると、著作権保護暗号を鍵Kkを用いて復号される。

【００６５】また、メタデータ暗号処理における特徴を以下に示す。第１に、送信側で著作権保護暗号方式のワーク鍵である鍵Kw2で暗号化されて配信される。著作権保護暗号方式の鍵Kkはメタデータの中に記入されるので、メタデータは著作権保護暗号方式のワーク鍵を用いて暗号化される。第２に、受信端末に受信されるとKw2を復号し、必要情報を抽出した後に、コンテンツ鍵Kkで再暗号後、ＨＤＤに蓄積される。鍵Kw2で暗号化されたままＨＤＤに蓄積しない理由は、鍵Kw2は、一定期間中は放送事業体に対して唯一であるので、同じ鍵で暗号化されたメタデータが複数存在する事になり、攻撃に対して強度が弱くなるという事と、鍵Kw2は定期的に変更されるので、当該メタデータが存在する限り、変更後も過去の鍵Kw2を保持する必要があるという理由等がある。

【００６６】４．受信端末

図９に、受信端末の基本構成図を示す。受信端末は（ＰＤＲ）２０、コンテンツ、メタデータ、番組配列情報であるPSI/SI等の各種データを受信を行う受信部２０３と、送信側のMUXで多重化されたデータを、多重化する前の状態に一連のデータに戻すDEMUX２０４と、受信したコンテンツ、メタデータ等のデータを蓄積する大容量蓄積媒体（ＨＤＤ等）２０５と、限定受信方式に関係する処理を行う際に必要な情報を格納する、従来（BS/CSデジタル放送）のICカードもしくは、同機能を備えたチップを想定したＣＡＳ用カード（ＣＡモジュール１）２０１と、可搬性を持たせ個人で携帯し、個人認証や視聴契約等の処理を行う際に必要な情報を格納するＲＭＰ用カード２０２（ＣＡモジュール２）と、コンテンツの著作権、権利保護機能であるＲＭＰ２００等を備える。

【００６７】図１０に、ＰＤＲ内における機能ブロック図を示す。リアルタイム型では、既存型放送コンテンツは受信処理２１０により受信され限定受信方式（ＣＡＳ）２１１の暗号を復号し、リアルタイムで再生される。次に、蓄積型では、サーバー型放送コンテンツの処理を示す。まず、嗜好アプリケーション２１６は、ユー

ザーインタフェースにより入力された情報や、視聴履歴情報等を基にユーザーの嗜好を判断する。嗜好性アプリケーション２１６に入力する情報は、例えば、視聴履歴としては、視聴コンテンツのジャンル、キーワード等、また、ユーザーインタフェースによる入力としては、趣味、特技等がある。嗜好性アプリケーション２１６は、上記情報よりユーザー嗜好性情報を作成する。その後、ＲＭＰ２１２から認証された後にアクセス可能となるＨＤＤ２１３内の一部のエリアに蓄積されているEPGテーブル、検索テーブル等を見て、ユーザーの嗜好にあったコンテンツを選定する。ユーザー嗜好性情報は、コンテンツのジャンルやキーワードに沿ったフォーマットで作成される。また、ユーザー嗜好性情報を作成する上で、登場回数の多い単語は優先度を高く設定する。さらに嗜好性アプリケーション２１６は、EPGテーブルに格納されている各EPG情報のジャンルやキーワード等と、作成したユーザー嗜好性情報とを比較して（検索を行い）、一致（あいまい一致）したコンテンツをユーザー嗜好性に沿ったコンテンツとみなして蓄積予約（嗜好性の優先度が高いコンテンツから蓄積予約）する。なお、ＨＤＤ２１４のコンテンツ、メタデータ等は、嗜好性アプリケーション２１６からアクセス不可である。一方、ＨＤＤ２１３のEPGテーブル、検索テーブル等は嗜好性アプリケーション２１６からアクセス可能である。そのユーザー嗜好にも優先度を設定し、より優先度が高いコンテンツから優先的に選定することも可能である。スケジュール管理としては、嗜好性アプリケーション２１６等により選定された一つ、もしくは複数のコンテンツの予約録画スケジュールを組み、そのスケジュールに従って、受信処理２１０を行なう機能に対して、コンテンツのIDやメタデータのIDや放送時間等の受信に必要な情報を渡す。嗜好アプリケーション２１６が受信処理２１０機能に対して受信要求を出すタイミングは、コンテンツの放送時間より前もって録画予約という情報を渡したり、コンテンツの放送時間に嗜好アプリケーションが判断をして録画指示を出すことも可能である。嗜好アプリケーション２１６がスケジュールを組む際、ＰＤＲ内に存在するチューナの個数によってスケジュールの組み方が変化する。それは、チューナの個数に対応して同時にＨＤＤに蓄積可能なコンテンツの個数が変化するからであり、例えば、ＰＤＲ内に複数チューナが存在すれば、同時に複数のコンテンツを蓄積可能となり、時間的に重複したコンテンツをスケジューリングする事が可能となる。受信処理２１０機能は嗜好アプリケーション２１６から渡されたスケジュール情報を基に、コンテンツとメタデータの蓄積処理を行う。まず、スケジュールによって蓄積指示が出ているメタデータをＲＭＰ２１２で取得し、そこで、暗号化メタデータを復号し権利情報等、蓄積時に必要な情報を基に蓄積可能か判断する。蓄積可能と判断した時は、メタデータの情報より、セットのコンテンツをＲＭＰ２１２に読み込み、メタデータを再暗号化した後に、コンテンツとメタデータをＨＤＤ２１４に蓄積する。その後、ユーザーが視聴コンテンツを選択した時に、始めにメタデータをＲＭＰ２１５に読み込み、そこで、視聴契約処理及び課金処理等を行う。その後、コンテンツをＲＭＰ２１５に読み込んで、ＲＭＰ２１５により復号した後にコンテンツの再生となる。

【００６８】５．ＲＭＰ

（ＲＭＰにおける暗号処理）図１１に、ＲＭＰ内における暗号処理の構成図を示す。本総合データ配信サービスにおける暗号方式は、限定受信方式と著作権保護暗号方式が想定される。例として、限定受信暗号と著作権保護暗号がかかっている暗号方式と、著作権保護暗号のみかかっている暗号方式の暗号処理を示す。限定受信暗号と著作権保護暗号がかかっている時は、コンテンツは、受信部を通った後、限定受信暗号デスクランブラ２５０で復号された後、ＨＤＤ２５１に蓄積される。ユーザーが視聴コンテンツを決定すると、著作権保護暗号デスクランブラ２５２で復号された後、デコーダにより再生され視聴可能となる。著作権保護暗号のみの場合は、コンテンツは受信部を通った後、ＨＤＤ２５１に蓄積される。そして、ユーザーが視聴コンテンツを決定すると、著作権保護暗号デスクランブラ２５２で復号された後、デコーダにより再生され視聴可能となる。

【００６９】（ＲＭＰの機能）ＲＭＰ内の各機能を以下に示す。ＲＭＰコントローラー、受信制御、蓄積制御、コピー制御、視聴制御、課金制御、暗号化、復号化、個人認証制御、時刻管理、視聴履歴制御、外部機器認証、通信制御、検索制御、Plug In アプリケーション認証制御、メタデータ制御、プロファイル制御、ICカード制御、鍵制御等の機能が考えられる。

【００７０】図１２に、ＲＭＰ内の機能構成図を示す。以下に各機能について説明する。ＲＭＰコントローラとは、ＲＭＰ内部で行なわれる処理等を制御管理する機能である。その主な機能は、ＲＭＰ外部とのI/F機能（デコーダ、アプリケーション、制御マネージャ等）と、ＲＭＰ内部の各機能の制御管理（コントロール）等である。受信制御とは、取得したPSI/SIやメタデータよりサービスの種別等を判断し、ＲＭＰ内部での復号処理の選択等を行なう機能である。主な機能は、PSI/SIよりコンテンツ、メタデータの取得経路の選択と、PSI/SIよりコンテンツ、メタデータの復号処理の選択、必要に応じてPSI/SIよりメタデータに追記する情報を生成等である。

【００７１】蓄積制御とは、ＲＭＰ内部で発生するコンテンツ、メタデータ等の蓄積媒体への蓄積動作をメタデータ、プロファイルの情報により制御する機能である。主な機能は、全体プロファイルの情報より、コンテンツの蓄積指示（録画予約等）が出ているか判定と、メタデータの情報より、コンテンツが蓄積可能かを判定と、コンテンツ、メタデータの蓄積媒体への蓄積指示等であ

る。コピー制御とは、視聴契約等のユーザーリクエスト等により発生するコピー要求をメタデータの情報により制御する機能である。主な機能は、メタデータの情報よりコンテンツのコピーが可能かを判定と、コンテンツ(Kk)、コンテンツ(Ks)、のコピー指示等である。

【００７２】視聴制御とは、ユーザーの視聴要求に対しメタデータの著作権、権利情報等よりＲＭＰ内でのコンテンツの再生を制御する機能である。主な機能は、メタデータの著作権、権利情報とＲＭＰ用カードの個人情報の比較により、ユーザーがアクセス可能なコンテンツか判定と、メタデータの著作権、権利情報とユーザーリクエスト情報の比較により、ユーザーが視聴可能なコンテンツか判定と、コンテンツの視聴契約処理と、視聴情報、契約情報の生成と、ＲＭＰと再生アプリケーションのマッチングである。課金制御とは、視聴契約等により起こる課金処理を、メタデータ内の契約条件及びユーザーの契約条件選択により制御する機能である。主な機能は、契約情報に基づき、課金処理と、課金情報の生成等である。

【００７３】暗号化機能とは、受信端末内部でのメタデータの暗号化を制御する機能である。主な機能は、メタデータの暗号化等である。復号化機能とは、ＲＭＰ内部でのコンテンツ、メタデータの復号化を制御する機能である。主な機能は、限定受信方式暗号の復号と、著作権保護暗号（暗号化コンテンツ、暗号化メタデータ）の復号等である。

【００７４】個人認証機能とは、ユーザー、ＲＭＰ用カード、個人プロファイル間の認証を行う機能である。主な機能は、受信端末にICカードを挿入し、パスワードを入力する事により、ユーザーとＲＭＰ用カードの認証と、受信端末にＲＭＰ用カードを挿入する事により、ＲＭＰ用カードと個人プロファイルの認証と、個人プロファイル内のパスワードによりユーザーの識別等である。時刻管理とは、コンテンツ復号時等の有効期限の確認において正確な時間（ユーザーによる時刻情報の改ざん等を防ぐ）を提示するための機能である。主な機能を以下に示す。TOT等の情報より、時刻の補正と、受信端末内の現在時刻を一元管理等である。よって、ユーザーが日時を設定する必要がなくなり、日時設定のユーザーインターフェースを用意しない事も可能となり、ユーザーによる故意の時刻情報の変更等による、有効期限等の時間に関する権利の保護が可能となる。TOT等の時刻情報自体も暗号化され配信されることもある。

【００７５】視聴履歴制御とは、個人プロファイルに格納されている視聴情報より、視聴履歴や嗜好性情報を生成する機能である。主な機能は、個人プロファイルの視聴情報より、視聴履歴情報を作成と、視聴履歴情報より、ユーザー嗜好性情報を作成等である。外部機器認証機能とは、蓄積、コピー、再生等の目的で外部機器を接続する際に、その外部機器の著作権保護レベル、不正機器等を識別する機能である。主な機能は、メタデータ内の情報に基づき、外部機器の著作権保護機能の認証等である。

【００７６】通信制御とは、視聴履歴収集、課金情報収集等外部回線を利用し著作権もしくはプライバシーに関わるデータを送受信する際の通信路の安全性に関する制御を行なう機能である。主な機能は、ＲＭＰとモデム等の回線終端を行い、回線の接続や切断を確実に行う回線制御、送受信間で同期を取り合う同期制御、データ通信の途中で発生しうるデータの誤りをチェックし、誤りを発見したときはそれを訂正する誤り制御等の伝送制御と、公開鍵方式を用いた認証処理等である。検索制御とは、蓄積媒体内の指定されたデータの検索とＲＭＰへ読み込む機能である。主な機能は、検索時、視聴契約時、視聴時、リムーバブルメディア蓄積時等に、ＨＤＤ内もしくはリムーバブルメディア内等から、目的のコンテンツもしくはメタデータをＲＭＰ内に読み込む事である。

【００７７】Plug In アプリケーション認証制御とは、ＰＤＲにPlug Inされたアプリケーションと認証を行い、認められたアプリケーションのみＲＭＰとアクセス可能とする機能である。主な機能は、Plug In アプリケーションの認証処理等である。メタデータ制御とは、メタデータに対して、ＲＭＰ内での受信処理、蓄積処理等の各処理を行なう際に必要となるデータの抽出、及び各処理時に生成される情報の格納を制御する機能である。主な機能は、蓄積処理、視聴契約処理、検索処理等の各処理を行なう際に必要となる情報をメタデータから抽出と、受信処理、視聴処理等に生成される情報をメタデータの該当部分へ格納と、メタデータの分割等である。

【００７８】プロファイル制御とは、全体プロファイル、個人プロファイルを管理しＲＭＰ内の各処理を行なう際に必要となるデータのプロファイルからの抽出、生成された情報のプロファイルへの格納（EMM2、ＲＭＰ用ICカード等の情報による受信端末内のユーザー環境設定等も含む）を制御する機能である。主な機能は、個人契約、全体契約の契約情報を管理と、個人ID、グループID等の個人情報を管理と、視聴履歴情報の管理と、録画予約等のスケジュールを管理等である。ICカード制御とは、各処理におけるＣＡＳ用カード、ＲＭＰ用カードに対するアクセスを制御する機能である。主な機能は、EMM1、ECM1の情報をＣＡＳ用カードに格納指示と、ＣＡＳ用カードからスクランブル鍵Ksの掃出指示と、ＲＭＰ用カードの個人情報より個人認証等がある。鍵制御とは、ＲＭＰ内部での鍵生成、鍵管理を制御する機能である。主な機能は、鍵テーブルの制御等である。

６．受信端末（ＰＤＲ）で使用される情報

【００７９】本発明で示している総合データ配信サービスは、個人用可搬ＣＡモジュール２を用いて、個人単位の視聴契約、課金処理等の個人の概念と、ＣＡモジュール２を携帯してKIOSK端末でのコンテンツ購入、料金の

支払い、視聴履歴情報の伝送や他受信端末でのコンテンツの視聴等の可搬の概念を持ったサービスを想定している。よって受信端末内に常時格納されるべき情報および、可搬されるべき情報が存在する。

【００８０】ＲＭＰの処理の際に必要な情報は、メタデータ、全体プロファイル、鍵テーブル、ＣＡＳ用カード、ＲＭＰ用カード、検索テーブル等である。以下これら各情報について説明する。なお、上記以外にも、ＰＤＲを個人用の環境に設定するために用いられる個人プロファイルの概念があり、その情報はユーザーがＲＭＰを挿入するたびに、ＲＭＰ用カードから必要な情報を入手し、個人プロファイルを生成する。しかし、個人プロファイルを用意せずに、随時ＲＭＰ用カードから必要な情報を入手することも可能である。ＰＤＲ固定情報は全体プロファイル、鍵テーブル、ＣＡＳ用カード、検索テーブル等である。ＰＤＲより可搬可能な情報はＲＭＰ用カード等である。

【００８１】（ＣＡＳ用カード（ＣＡカード１））図３５に、ＰＤＲに常時固定させる必要がある情報の説明図を示す。すなわち、図３５(Ａ)に、本発明の権利保護システムにおいて新規で追加した情報を示し、図３５(Ｂ)に、従来（２０００年１２月からサービスインのBSデジタル放送）のデジタル放送において限定受信用として用いられている情報を示す。これらは受信端末内に固定で格納される情報である。このようにＣＡＳ用カードは、BS放送のＣＡＳ用ICカードと同じ情報を格納するため、コンテンツの受信に関する情報等が格納されている。

【００８２】（ＲＭＰ用カード（ＣＡカード２））図３６に、ＰＤＲより可搬させることが可能な情報の説明図を示す。これは本発明の権利保護システムにおける新しい概念である可搬性のあるＲＭＰ用カードに格納する情報である。このようにＲＭＰ用カードは、受信端末を利用するユーザー毎に用意され、個人の情報、契約済みコンテンツの視聴契約情報等が格納される。ＲＭＰ用カードを受信端末に挿入すると、全体プロファイルに記載してある、グループ契約におけるグループ員による契約済みコンテンツの視聴契約情報等の必要情報がＲＭＰ用カードに記入される。その後、受信端末内をユーザー個人の環境にするため、ＲＭＰ用カード内の必要な情報をＲＭＰ内に読み込み、個人プロファイルに展開する。しかし、個人プロファイルに展開せずに、随時ＲＭＰ用カードにアクセスして情報を入手する事も可能である。

【００８３】（メタデータ）コンテンツの関連情報が記載されているメタデータは、ＲＭＰの処理おいては不可欠である。メタデータに記載してある著作権、権利情報等を見て、コンテンツに対する処理方法が変わる。このメタデータに記載されている情報は暗号をかけて守るべき情報も含まれている。メタデータの詳細は前述の通りである。

【００８４】（全体プロファイル）図３７に、全体プロファイルの主な項目、内容の説明図を示す。主に受信端末を利用するユーザー全体に関わる端末情報、コンテンツの蓄積予約、視聴予約等のスケジュールに関する情報および各個人の情報を纏めたグループ情報であるＰＤＲ設定情報等が格納される。

【００８５】（鍵テーブル・検索テーブル）図３８に、鍵テーブルと検索テーブルの内容についての説明図を示す。鍵テーブルは、図３８(Ａ)のように、受信端末内部で保管管理する鍵の情報等が格納される。その中には鍵Kw2、Kk、Kmc用の3種類が存在する。但し鍵Kmcは受信端末に対して唯一もしくは全ての受信端末で共通であるため鍵、自体のみを格納している。検索テーブルは、図３８(Ｂ)のように、各処理においてコンテンツ、メタデータの蓄積場所を識別する際に必要となる情報が格納されている。概要は容量等の問題から必要に応じて用いられる。

【００８６】（ＲＭＰの機能と情報の関係）図３９に、ＲＭＰの各機能とその際に用いられる情報エリアの関係図の一例を示す。必ずしも、このような関係が成り立つ訳ではなく、各処理手順によって、例外が生じる可能性がある。例えば、②蓄積制御では、メタデータと全体プロファイルが用いられ、④視聴制御では、メタデータ、個人プロファイル及びＣＡカード２(ＲＭＰ用カード)が用いられる。

【００８７】７．受信端末（ＰＤＲ）アプリケーション

以下にＰＤＲに関する各アプリケーションについて説明する。

（検索アプリケーション）検索アプリケーションは、蓄積視聴において、蓄積装置に蓄積されているコンテンツの中から視聴を望むコンテンツを選択する際の手助けをする機能を持つ。検索処理を行うための各コンテンツについての情報は、検索テーブルおよびメタデータから入手する。検索処理によって選択されたコンテンツ情報（コンテンツのロケーション、メタデータのロケーション等）はＲＭＰに渡され、ＲＭＰが蓄積装置にアクセスし、データをＲＭＰ内に読み込む。検索対象は、ＨＤＤ等の蓄積媒体に蓄積されているコンテンツのみだけでなく、将来配信される予定のコンテンツ情報を入手し、検索をする事も可能である。例として、EPG用として配信された情報を入手し、キーワード、タイトル、ジャンル等で検索を行い、録画予約を行うことも可能である。

【００８８】（基本処理手順）図１３に、受信端末における、コンテンツ受信から視聴までの基本処理フローチャートを示す。処理手順は、受信処理（S1301）、限定受信暗号の復号処理（S1303）、蓄積処理（S1305）、検索処理（S1307）、視聴契約処理（S1309）、課金処理（S1311）、メタデータ処理（S1313）、コンテンツ復号処理（S1315）の順で行われる。以下各処理について、詳細に説明する。

【００８９】（S1301,受信処理）図１４に、受信処理の

処理手順と、配信時における暗号方式と蓄積時における暗号形態の関係を示す。配信されたデータの暗号方式として以下の場合が考えられる。
CASE１：限定受信方式＋著作権保護暗号方式
CASE２：限定受信方式
CASE３：著作権保護暗号方式
CASE４：暗号化なし
【００９０】受信端末がコンテンツを受信した際、ＨＤＤ蓄積時の暗号形態を認識し、それぞれの場合における復号処理手順を選択する。コンテンツの蓄積時における暗号形態として、コンテンツに限定受信方式をかけたまま蓄積する限定受信方式蓄積と、著作権保護暗号でコンテンツが暗号化されている状態で蓄積する著作権保護暗号方式と、暗号化されていない状態で蓄積する暗号なし蓄積が考えられる。
【００９１】（S1303,限定受信暗号の復号処理）図１５に、伝送路暗号の復号処理手順を示す。受信制御機能で識別した復号処理手順に従って復号を行う。それぞれの蓄積時暗号方式の場合の復号処理手順を以下に示す。
・限定受信方式蓄積：メタデータのみ、限定受信暗号を復号
・著作権保護暗号方式蓄積：
CASE１：コンテンツ、メタデータ両方の限定受信暗号復号
CASE３：処理なし
・暗号なし蓄積：コンテンツ、メタデータ両方の限定受信暗号復号
【００９２】（S1305、蓄積処理）図１６及び図１７に、蓄積処理の処理手順を示す。このステップでは、伝送路暗号を復号した後から、ＨＤＤに蓄積するまでの処理を行う。主な処理手順を以下に示す。
・メタデータ復号３００
・検索テーブルにメタデータの検索、権利情報の一部を記入３０１
・メタデータから鍵Kk入手３０２
・メタデータ暗号化３０３
【００９３】（S1307,検索処理）図１８、図１９に、検索処理の処理手順を示す。検索処理は、視聴もしくはリムーバブルメディアに蓄積するコンテンツを、選択する際の処理である。検索処理は受信端末のアプリケーションである検索アプリケーションが行い３１０、ＨＤＤからＲＭＰ内へのデータの読み込みはＲＭＰの視聴制御が行う３１１。ユーザーリクエストによりＨＤＤ内のコンテンツを検索し、検索結果を提示する。提示する内容は、以下のように詳細度によって２段階とする。
①検索テーブルの情報により、コンテンツのタイトル、番組概要等の概略情報
②メタデータの情報により、番組の詳細な内容、料金等の詳細情報
【００９４】（S1309,視聴契約処理）図２０に視聴契約処理の処理手順を示す。ユーザーがコンテンツの視聴契約の際に入力・確認した情報を基に、視聴契約処理を行う。ユーザーに対して、メタデータの契約情報を提示し３２０、アクセス権、視聴条件等を考慮し、そのユーザーがコンテンツ視聴可能かを判断する３２１、３２２。
【００９５】（S1311,課金処理）図２１に、課金処理の処理手順を示す。ここでは、視聴契約をおこなったコンテンツに対して、契約情報に基づいて課金処理を行う。課金処理結果の情報である課金情報と視聴情報、契約情報、課金情報をまとめた視聴契約情報は必要であれば全体プロファイルに格納される３３１。
【００９６】（S1313,メタデータ処理）図２２に、メタデータ処理の処理手順を示す。ここでは、視聴契約処理、課金処理等、契約に関わる処理が済んだ後、それらの情報をまとめた視聴契約情報をメタデータに記入し、そのメタデータを加工処理する。主な処理手順を以下に示す。
・メタデータに視聴契約情報を記入３４０
・視聴契約情報、Kk等をＲＭＰカードに格納３４１
・必要であれば、ＲＭＰカード内を鍵Km2で暗号化３４２
【００９７】（S1315,コンテンツ復号処理）図２３、図２４に、コンテンツ復号処理の処理手順を示す。ここでは、視聴契約が行われたコンテンツを視聴する際に、暗号化されたコンテンツを復号する。コンテンツ暗号の鍵Kkは個人プロファイルに格納されている。鍵Kkを入手し、コンテンツを復号する手順を以下に示す。
・ＲＭＰ用カード情報から生成された個人プロファイルの鍵KkでＨＤＤ内のメタデータを復号３５０
・ユーザー制限の判断３５１
・個人プロファイルのKkでＨＤＤ内のコンテンツ復号３５２
【００９８】（メタデータを用いたコンテンツ鍵伝送モデルにおける蓄積）図４３に、メタデータを用いたコンテンツ鍵伝送方式における処理手順の説明図を示す。また、図４４に、コンテンツ鍵伝送方式における処理手順のフローチャートを示す。以下に、メタデータを用いたコンテンツ鍵伝送方式における処理手順を説明する。まず初めにKs、Kw1とＣＡモジュール１に蓄積されているKm1を用いてBS伝送路スクランブルを復号し（５００）、暗号化コンテンツ４０１、暗号化メタデータ４５１を入手する。この場合、暗号化メタデータ４５１には、コンテンツ鍵Kkが含まれる。次に、予め受信端末（PDR）３に伝送され暗号/復号化モジュール内のRAM４５２に格納されているワーク鍵Kw2を用いてメタデータ４５１を復号し（５０３,４５３）、メタデータに記載されている検索/課金情報などの検索処理に用いられる情報を抽出し検索テーブル４１０に追加する（５０４）。この検索テーブル４１０はＨＤＤ４内のコンテンツ４０６の検索/課金情報が記載されていて、検索をする際に使用され

る。メタデータから検索処理に用いられる情報を抽出し検索テーブルに追記した後、暗号/復号化モジュール内で生成もしくは用意させた値Ktを鍵Kt４５３として（５０６）、Kw2で一度復号されたメタデータをKtで再暗号化４５３し（５０７）、Ktで暗号化されたメタデータ４０５を生成する（４５３）。鍵Ktは暗号/復号化モジュール内のRAM４５２に格納される。この鍵Ktは、メタデータ４５１をＨＤＤ４蓄積前に復号し再暗号化４５３する度に暗号/復号化モジュール内で生成もしくは用意させる鍵である。その後、コンテンツ鍵Kkで暗号化された暗号化コンテンツ４０６と鍵Ktで暗号化された暗号化メタデータ４０５をセットでＨＤＤ４に蓄積する（５０８）。なお、メタデータ４１４毎に異なる鍵としてもよい。

【００９９】（リムーバブルメディアへのコンテンツ蓄積）図４５に、リムーバブルメディアへのコンテンツ蓄積処理手順のフローチャートを示す。以下に、ＨＤＤ４に蓄積されたコンテンツ４０６をリムーバブルメディア５に蓄積するまでの処理手順を説明する。図４３を参照して、リムーバブルメディアへのコンテンツ蓄積処理について説明する。

【０１００】ユーザーがキーワード等を入力することにより、検索テーブル４１０の情報を基にＨＤＤ４内の検索処理４１２が行われる（５２０）。その検索結果より、ユーザーが蓄積コンテンツ４０９を選択する（５２０）。そして、選択されたコンテンツ４０９に対するメタデータ４０８を受信端末（PDR）３内のワークエリアにコピーする。コピーされたメタデータ４０８を鍵Ktを用いて復号４１３する（５２２）。そして、ユーザーが、選択したコンテンツ４０８の契約条件を確認後必要な情報を追記し、蓄積を決定４１５する（５２３）。ユーザーの蓄積決定の動作を受けて、ユーザーが契約した契約条件より課金処理４１６が行われる（５２４）。契約条件、課金処理の結果より、メタデータ４１４の契約情報を作成する（５２５）。その後、メタデータ４１４をメタデータ１、２に分離する（５２６）。そして、受信端末（PDR）３内で生成もしくは用意させた値Kt'を鍵Kt'４１８とする（５２７）。この鍵Kt'は、コンテンツ４０９の視聴手続き後、メタデータ２をリムーバブルメディア５、ＨＤＤ４等に蓄積前に暗号化する度に受信端末（PDR）３内で生成もしくは用意させる鍵である。メタデータ２を鍵Kt'で暗号化し（５２８）、リムーバブルメディア５に蓄積する（５２９）。次に、メタデータ１に鍵Kt'もしくは、鍵に関する情報を記入する。メタデータ１をセキュリティが守られている伝送路を用いてＣＡモジュール２　１０１に蓄積し（５３１）、ＣＡモジュール２　１０１に蓄積されている個人鍵Km2　４２４を用いて暗号化４２２する（５３０）。この処理において、セキュリティが守られている伝送路を用いて個人鍵Km2　４２４を受信端末（PDR）３内に入力し、鍵Kt'もしくは鍵Kt'に関する情報を含んでいるメタデータ１を個人鍵Km2４２４を用いて暗号化した（４２２、５３０）後、ＣＡモジュール２　１０１に蓄積する（５３１）事も可能である。またこれ以外の方法として、セキュリティが守られた伝送路で鍵Kt'もしくは鍵Kt'に関する情報を含んでいるメタデータ１をＣＡモジュール２１０１に伝送し、そのまま保存する場合もある。メタデータ４１４に関する処理が全て完了したら、暗号化コンテンツ４０９をリムーバブルメディア５に蓄積する（５３２）。このようにして、リムーバブルメディアに格納される情報は、鍵Kk'で暗号化され鍵Kkを含むメタデータ２　４２１、鍵Kkで暗号化されたコンテンツ４２７となる。

【０１０１】（コンテンツ視聴）図４６に、コンテンツ視聴処理手順のフローチャートを示す。また、図４７に、メタデータを用いた蓄積後視聴のデータの流れについての説明図を示す。以下に、図４３を参照して、ＨＤＤ４に蓄積されたコンテンツ４０８を視聴するまでの処理手順を説明する。ＨＤＤ４には、鍵Kkを含む暗号にメタデータと暗号化コンテンツが記帳されている。ユーザーがキーワード等を入力することにより、検索テーブル４１０の情報を基にＨＤＤ４内の検索処理４１２が行われる（５２０）。その検索結果より、ユーザーが視聴コンテンツ４０９を選択する（５４０）。そして、選択されたコンテンツ４０９に対するメタデータ４０８を受信端末（PDR）３内のワークエリアにコピーする。

【０１０２】メタデータについては、次のように処理される。コピーされたメタデータ４０８を鍵Ktを用いて復号４１３する（５２２）。そして、ユーザーが、選択したコンテンツ４０９の契約条件を確認後、視聴を決定４１５する（５４１）。ユーザーの視聴決定の動作を受けて、ユーザーが確認、契約した契約条件より課金処理４１６が行われる（５２４）。契約条件、課金処理の結果より、メタデータの契約情報を作成４１７する（５２５）。その後、メタデータ４１４をメタデータ１、２に分離する（５２６）。そして、受信端末（PDR）３内で生成もしくは用意させた値Kt'を鍵Kt'とする（５２７）。この鍵Kt'は、コンテンツ４０９の視聴手続き後、メタデータ４１４をリムーバブルメディア５、ＨＤＤ４等に蓄積する前に暗号化する度に受信端末（PDR）３内で生成もしくは用意させる鍵である（なお、メタデータ４１４毎に異なる鍵としてもよい）。次に、メタデータ２を鍵Kt'で暗号化４１９し（５２８）、ＨＤＤに蓄積する（５４２）。次に、セキュリティが守られている伝送路を用いて個人鍵Km2　４２４を受信端末（PDR）３内に入力し、鍵Kt'もしくは鍵Kt'に関する情報を含むメタデータ１を個人鍵Km2　４２４を用いて暗号化４２２した（５３０）後、ＣＡモジュール２　１０１に蓄積する（５３１）。この処理において、メタデータ１に鍵Kt'もしくは鍵Kt'に関する情報を記入する。メタデータ１をセキュリティが守られている伝送路を用いてＣＡモ

ジュール２　１０１に蓄積し（５３１）、ＣＡモジュール２　１０１に蓄積されている個人鍵Km2　４２４を用いて暗号化４２２する（５３０）。またこれ以外の方法として、セキュリティが守られた伝送路で鍵Kt'もしくは鍵Kt'に関する情報を含むメタデータ１をＣＡモジュール2　１０１に伝送し、そのまま保存する場合もある。一方、コンテンツについては、次のように処理される。メタデータ４１４に関する処理が全て完了したら、コンテンツ鍵Kk３３０を用いて暗号化コンテンツ４０９を復号４２６し（５４３）、視聴可能なコンテンツを入手する。

【０１０３】つぎに、図４８に、リムーバブルメディアに蓄積後視聴のデータの流れについての説明図を示す。リームバブルメディア５からの視聴処理についてもこのHDD４からのコンテンツの視聴処理と同様な処理が行なわれる。ただし、ここでは、ＣＡモジュール２　１０１に蓄積されたメタデータ１と、リムーバブルメディア５の蓄積されたメタデータ２との一致確認及び契約条件確認が行われた後、コンテンツの視聴（復号）が可能となる。暗号化メタデータ１は、セキュリティが守られている伝送路を用いて個人鍵Km2　４２４を受信端末３内に入力し復号することができる。復号化されたメタデータ1内の鍵Kt'を用いて、暗号化メタデータ２が復号化されることができる。メタデータ２内に格納されているコンテンツ鍵Kkにより、暗号化コンテンツを復号し、視聴可能となる。

【０１０４】８．視聴契約をおこなった受信端末以外におけるコンテンツ視聴

視聴契約を行った受信端末以外で、コンテンツを視聴する場合について以下に示す。視聴対象と契約コンテンツの移動の関係については、視聴対象が契約者のとき、契約コンテンツの移動ありまたはなしの場合があり、視聴対象が第３者のとき契約コンテンツの移動ありの場合等がある。以下視聴に関する各場合について説明する。

【０１０５】（契約者視聴）まず、視聴契約を行ったユーザーが、コンテンツを視聴する場合について示す。また、図４０に、上で述べた内蔵ＨＤＤ蓄積における基本処理手順との相違点の説明図を示す。

【０１０６】①契約済みコンテンツの移動による受信端末外視聴

図２５に、契約コンテンツの移動ありで契約者視聴の場合の説明図を示す。ここでは、契約済みコンテンツを、ＲＭＰ用カード及びリムーバブルメディアを用いて視聴契約を行った受信端末外で視聴する場合を示した。図４０(Ａ)のように、視聴契約処理、メタデータ処理、リムーバブルメディア蓄積及びコンテンツ復号が行われる。

【０１０７】②コンテンツの移動を伴わない受信端末外視聴

図２６に、契約コンテンツの移動なしで契約者視聴の場合の説明図を示す。ここでは、本人所有の受信端末ＲＭＰ１を用いてコンテンツの視聴契約を行い、コンテンツ自体を移動させず、視聴契約を行ったＲＭＰ用カードとＲＭＰ用カードの中に蓄積されている視聴契約情報やコンテンツ鍵Kk等のみを持ち運び、移動先の他の受信端末ＲＭＰ２内のコンテンツを視聴する場合を示す。このサービスは移動先の受信端末ＲＭＰ２内に契約コンテンツと同一のコンテンツが蓄積されている時のみ有効である。図４０(Ｂ)のように、メタデータ処理、コンテンツ復号が行われる。

【０１０８】③第３者視聴

（ギフトサービス）受信端末外において、契約済みコンテンツを契約者以外の第３者が視聴するサービスとして、ギフトサービスが考えられる。図２８は、通常サービスとギフトサービスの相違点を示す図である。まず、ギフト契約について説明する。ギフトとは、購入者が他人が保有する受信端末に購入したコンテンツを贈ることを指す。ＩＣカードは基本的に個人単位で所有するものであり、他人に譲渡する事はできない。よって、リムーバブルメディアとＩＣカードがセットで視聴可能なシステムは用いる事ができず、リムーバブルメディア単体を譲渡するだけで成り立つシステムである必要がある。

【０１０９】図４１に、通常契約とギフト契約の、処理対象の相違点の説明図を示す。ギフト契約では、送り主が視聴契約処理、課金処理等を行う。しかし、所有者登録処理だけは行われずに配送され、ギフト契約後、初めて視聴手順を行ったＲＭＰ用カードを所有者とみなす。当該ＲＭＰ用カード所有者がコンテンツの権利条件を満たしていない場合は、エラーを返す。

【０１１０】つぎに、ギフト契約の鍵管理・送信方式について述べる。図２９に、リムーバブルメディアに格納される情報の概要図を示す。暗号化コンテンツの鍵Kkはメタデータに記入される。ギフトサービスは、リムーバブルメディア単体のみで成り立つシステムなので、コンテンツとメタデータは同じリムーバブルメディアに格納される事になる。そのため、鍵Kkを保護するためには、メタデータを暗号化する必要がある。その暗号化メタデータの鍵をそのまま送信する事はできないので、鍵Keyの管理・送信方法に工夫が必要である。そこで、以下、ギフト鍵方式、共通鍵方式について説明する。

【０１１１】図３０に、リムーバブルメディアに格納される情報を示す。まず、ギフト鍵方式について説明する。ギフトサービスの際の、暗号化メタデータの鍵を送信しない、もしくは鍵に関連する鍵情報のみを送信する方式をここでは、ギフト鍵方式と呼ぶ。リムーバブルメディアの中に格納される、鍵情報等のギフト鍵方式を実現させるために必要な情報を、ここではギフト情報と呼ぶ。

【０１１２】（１）ギフト鍵（固有鍵）方式

図４２に、ギフト鍵（固有鍵）の種類の説明図を示す。この場合、ギフト鍵は全ての受信端末が共通の鍵をＲＭ

Ｐ内に保持していて、セキュリティ的に守られている。全ての受信端末において同じギフト鍵が格納されているので、鍵そのものを伝送しなくても鍵の入手は可能である。

①全ての受信端末に共通な唯一な固有鍵

・リムーバブルメディアにギフト鍵情報を記入しない

・全ての受信端末に共通な唯一な固有鍵なので、ギフト契約のコンテンツと判断できれば、受け取り側のギフト鍵でメタデータの復号が可能

②全ての受信端末に共通な、任意に用いる事が可能な数種類の固有鍵

・リムーバブルメディアにギフト鍵情報を記入する

・全ての受信端末が同じ鍵を保持しているので、リムーバブルメディアに鍵ID等の鍵を認識可能な鍵情報を記入していれば受け取り側のギフト鍵でメタデータの復号が可能

③全ての受信端末に共通な、各サービスプロバイダ毎に指定の固有鍵

・リムーバブルメディアにギフト鍵情報を記入する

・全ての受信端末が同じ鍵を保持しているので、リムーバブルメディアに鍵ID等の鍵を認識可能な鍵情報、もしくはサービスプロバイダ名もしくはID等を記入していれば受け取り側のギフト鍵でメタデータの復号が可能

これら①～③の各方式に対する必要情報は、例えば、受信端末ではギフト鍵であり、リムーバブルメディアではギフト鍵情報（全ての受信端末に共通の固有鍵を用いる時は不要）である。

【０１１３】（２）ギフト鍵（任意鍵）方式

１つもしくは複数の値（初期値）を基に、一定のアルゴリズムに基づいて鍵を生成する。鍵生成アルゴリズムは全ての受信端末において同じであるので、鍵そのものを伝送しなくても、鍵生成アルゴリズムの初期値を伝送すれば、受け取り側で鍵を生成可能である。この場合の必要情報としては、例えば、受信端末では鍵生成アルゴリズムであり、リムーバブルメディアではギフト鍵情報（初期値）である。

【０１１４】（３）公開鍵方式

この形式では、各受信端末毎の秘密鍵、公開鍵を用いて、暗号化メタデータの鍵に配送相手の公開鍵暗号方式で暗号をかけ、受け取り側は自分の秘密鍵で復号する。配送相手の公開鍵を知る方法として、配送相手から直接情報を得る方法以外に、鍵管理センタにアクセスして配送相手の公開鍵を知る方法も考えられる。この場合、必要情報としては、受信端末では、秘密鍵、公開鍵、配送先の公開鍵、鍵管理センタアクセスサイト（鍵管理センタから配送相手の公開鍵を知る時のみ必要）であり、一方、センタでは、全ての受信端末の公開鍵（鍵管理センタから配送相手の公開鍵を知る時のみ必要）

【０１１５】（４）共通鍵方式

配送相手を鍵配送センタに知らせることにより、本人所有受信端末と配送相手所有受信端末にその暗号化メタデータの鍵の暗号化専用の鍵であるセッション鍵が配布される。センタから配布されるセッション鍵は、それぞれの受信端末の共通鍵を用いた共通鍵方式、もしくは、それぞれの受信端末の公開鍵を用いた公開鍵方式で暗号化されている。センタから配布されたセッション鍵を共通鍵として用い、暗号化メタデータの鍵の暗号化行う。受け取り側はセッション鍵で復号する。この場合必要情報としては、例えば、受信端末では、秘密鍵※１、公開鍵※１、センタとの共通鍵※２、鍵管理センタアクセスサイトである。センタでは、全ての受信端末の公開鍵※１、全ての受信端末の共通鍵※２、である。ただし、※１は、セッション鍵を公開鍵方式で暗号化する時に必要なものを示し、※２は、セッション鍵を共通鍵方式で暗号化する時に必要なものを示す。

【０１１６】（グループ契約サービス）基本的に、ＲＭＰ用カードを用いたコンテンツ視聴および課金対象は個人単位である。しかし、家族等のグループ単位を、コンテンツ視聴および課金対象としたサービスも考えられる。まず、グループ契約のコンテンツのＨＤＤ蓄積における特徴を以下に示す。

・全体プロファイルのグループ情報使用

・グループ契約の視聴契約情報は全体プロファイルに記入

・視聴の際は個人プロファイルに記入されている視聴契約情報を使用

・グループ契約済みのコンテンツをグループ員が視聴する時は、新たにマスターメタデータ（デフォルト）のコピーに視聴契約情報を記入

【０１１７】つぎに、グループ契約を行ったコンテンツをＨＤＤに蓄積し、グループ員がグループ契約が行われた当該コンテンツを視聴する場合の処理手順（例）を以下に示す。

Ｓ1.視聴者ＡのＩＣカードＡをＰＤＲに挿入

Ｓ2.視聴者Ａによる、視聴契約

Ｓ3.マスターメタデータ（デフォルト）のコピーと全体プロファイルに視聴契約情報記入

Ｓ4.視聴情報に基づき課金処理

Ｓ5.ＩＣカードＡにメタデータの一部を格納

Ｓ6.視聴者ＢのＩＣカードＢをＰＤＲに挿入

Ｓ7.全体プロファイルからグループ員が契約したグループ情報、視聴契約情報等の必要な情報をICカード１に格納

Ｓ8.ICカード１から視聴契約情報等の必要な情報を入手して個人プロファイルの生成

Ｓ9.視聴者Ｂによる、視聴契約済みコンテンツの視聴選択

Ｓ10.全体プロファイルのグループ情報より、視聴可能なユーザーがどうか確認

Ｓ11.視聴

【０１１８】つぎにグループ契約を行ったコンテンツをリムーバブルメディアに蓄積し、グループ員がグループ契約が行われた当該コンテンツを本人所有受信端末外で視聴する場合を示す。リムーバブルメディア蓄積の際の処理手順の変更点は、蓄積場所の変更のみである。蓄積場所がＨＤＤからリムーバブルメディアに変更になった際の追加条件・情報を以下に示す。すなわち、視聴契約をおこなった本人のみの視聴の条件は特にない。また、グループ員の視聴の条件は、次のようなものがある。

・リムーバブルメディア内に視聴情報の記入が必要

・リムーバブルメディア内に視聴可能なグループ員の記入が必要

・リムーバブルメディア内にマスターメタデータ（デフォルト）の蓄積が必要

・上記３つの情報を暗号化する鍵は、全ての受信端末共通の鍵か、リムーバブルメディアに鍵情報の記入が必要この場合の必要情報としては、例えば、受信端末では、受信端末共通の鍵であり、また、リムーバブルメディアでは、鍵情報、視聴契約情報、マスターメタデータ（デフォルト）、グループ情報である。

【０１１９】（公衆環境における視聴契約）受信端末外で視聴契約が行われる例として、KIOSK端末等の公衆環境にある端末によるコンテンツ購入がある。以下、KIOSK端末を例に説明する。KIOSK端末は、個人用のICカード（ＲＭＰカード（ＣＡカード２））を挿入することにより、不特定のユーザーが使用可能である。KIOSK端末内には、ユーザーが購入可能な暗号化コンテンツと、暗号化コンテンツの鍵が記入されているメタデータが格納されている。

【０１２０】図２７に、公衆環境における視聴契約の処理フローを示し、特徴を以下に示す。

・衛星回線、地上回線等を用いて、KIOSK端末にコンテンツ、メタデータが予め配信される。

・ユーザは、ICカードをKIOSK端末に挿入する（Ｓ１４０１）。

・KIOSK端末のモニター上で視聴コンテンツを検索する（Ｓ１４０３）。

・選択したコンテンツの視聴契約を行う（Ｓ１４０５）。

・ICカード、コンテンツを含むメディア媒体は持参をユーザが入手する（Ｓ１４０７）追加料金で購入可能。購入した場合、ICカードは臨時用使い捨てカードとなり、使用期限を設定することができる。

・KIOSK端末は、地上回線を用いて購入履歴等をセンターに送信し、顧客管理・センターは、地上回線を用いてKIOSK端末を制御する（コンテンツ削除、臨時用ICカード、メディア媒体の枚数管理等）。公衆環境に設置してあるKIOSK端末はコンテンツの購入以外にも、センタに課金情報の伝送や料金の支払いや、視聴契約情報の登録等が可能である。

・ユーザは、受信端末、移動体通信機器、携帯型受信機器等により、ICカードとメディア媒体を用いてコンテンツを視聴する（Ｓ１４０９）。

【０１２１】９．まとめ

本発明の特徴のいくつかを以下に例示する。

・衛星、地上回線等の通信回線もしくはリムーバブルメディア等のメディア媒体を用いて、家庭にコンテンツを配信し、家庭内でデジタルのまま蓄積/コピー/再生を行う際の、データの不正な書き換え、再生、私的利用を超えるコピー等のサービスプロバイダ、著作権所有者もしくはユーザーの権利、著作権を侵害する事態の回避のために、コンテンツの著作権者、放送事業者、視聴者など各々の権利を保護、管理を行うこと。

・コンテンツの著作権保護、権利保護処理機能の概念をＲＭＰ(Rights Management & Protection)とし、受信端末内に著作権保護、権利保護機能をもつこと。

・コンテンツの著作権保護もしくは権利保護方法のために、情報の不正な書き換えおよび視聴を防ぐ暗号化と、サービスプロバイダもしくは著作権所有者によるコンテンツへのユーザーアクセス制限権利と、ユーザーによるコンテンツ視聴権利の保護のための個人認証と、著作権情報もしくは権利情報等を格納するコンテンツ関連情報（メタデータ）および、デジタルの画像、ビデオ、音声等の中に情報をうめこむ電子すかし等を用いること。

【０１２２】・コンテンツとメタデータの暗号方式として、伝送路の暗号として用いる限定受信方式と、コンテンツとメタデータの著作権保護および権利保護の目的として使用される著作権保護暗号方式を用いること。

・蓄積視聴の際、既存型放送は伝送時の限定受信暗号をかけたまま蓄積し再生時に限定受信暗号を復号し、サーバー型放送は伝送時の限定受信暗号を復号後に、著作権保護暗号のみの状態で蓄積し、再生時に著作権保護暗号を復号すること。

・前記の著作権保護暗号方式におけるコンテンツとメタデータの暗号化は、サービスプロバイダの送信設備または鍵管理センタの設備で暗号化可能なこと。

【０１２３】・前記の著作権保護暗号方式におけるコンテンツとメタデータの暗号の鍵は鍵管理センタで管理すること。

・前記の著作権保護暗号方式において、コンテンツは伝送側で著作権保護暗号でコンテンツ鍵Kkを用いて暗号化し、受信側で同じ暗号方式と同じ鍵で蓄積すること。

・前記の著作権保護暗号方式において、コンテンツの暗号化の鍵であるコンテンツ鍵Kkはメタデータに格納されてコンテンツとセットで配信されること。

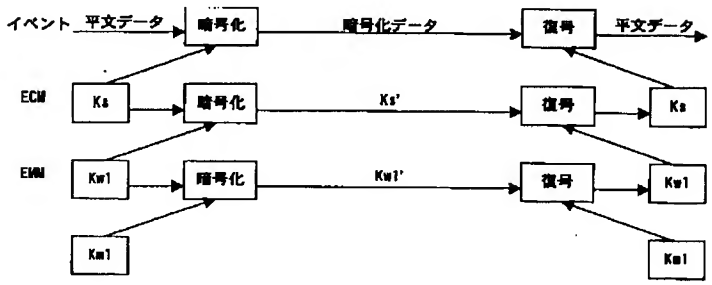
・前記の著作権保護暗号方式において、コンテンツの視聴契約が終わったら、コンテンツ鍵Kkを個人用可搬ＣＡモジュールに格納すること。

【０１２４】・前記の著作権保護暗号方式において、メタデータは保護が必要な情報のみ暗号化し、保護の必要

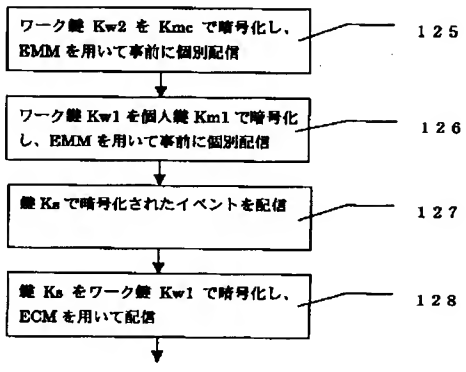
のない情報は暗号化しないこと。
・前記の著作権保護暗号方式において、メタデータは送信側で著作権保護暗号で暗号化し、受信端末に受信されると復号され必要情報およびコンテンツ鍵Kkを抽出し、新たに、コンテンツ鍵Kkで再暗号化されること。
・使用時に受信端末内を個人用の環境に設定するために、個人用環境情報エリアを設定しておき、各ユーザーが受信端末使用時に、個人用可搬ＣＡモジュールより個人用環境情報エリアの生成に必要な情報を取得し、個人用環境情報エリアを生成すること。
・個人用可搬ＣＡモジュール内に個人用環境情報エリアの生成に必要な情報とコンテンツ鍵Kkと視聴契約情報等が格納されていること。
【０１２５】・大容量蓄積装置に蓄積させる方法としてユーザーによる嗜好情報入力や視聴履歴情報の情報源としたユーザー嗜好性による蓄積や、SIやメタデータからの番組情報等を情報源としたEPGによる予約蓄積や、緊急時や特定時間帯もしくは、定められた容量内でサービスプロバイダが強制的に大容量蓄積媒体に蓄積する強制蓄積等があること。
・受信端末内に常時格納されるべき情報と可搬されるべき情報があり、常時格納されるべき情報として各個人の情報をまとめたグループ情報等や現状の限定受信方式に使用されている情報等があり、可搬されるべき情報としてKIOSK端末におけるコンテンツ購入、料金の支払い視聴履歴情報の登録、他受信端末でのコンテンツ視聴等に必要な情報であること。
・個人用可搬ＣＡモジュールに視聴履歴情報、コンテンツ鍵Kk等を格納することにより、視聴契約をおこなったコンテンツと同一コンテンツが他の受信端末に蓄積されている際に、再び視聴契約を行わずに視聴が可能であること。
【０１２６】・第3者に対して視聴契約済みコンテンツを贈呈するいわゆるギフト契約の時、個人用可搬ＣＡモジュールを渡さずに、リムーバブルメディア内に視聴契約済みコンテンツと、鍵情報と視聴契約情報等を格納したり、共通鍵方式もしくは公開鍵方式を用いてコンテンツ鍵を格納しているメタデータの鍵を暗号化して、リムーバブルメディアのみを用いて視聴可能となること。
・視聴契約単位や課金単位を個人単位ではなくグループ単位で設定するいわゆるグループ契約の時、グループ全員の情報を纏めたエリアを設定し、そこに視聴契約情報等を格納することによりグループ員全員で視聴契約済みコンテンツの共有化が可能となること。
【０１２７】
【発明の効果】本発明によると、暗号化、個人認証、メタデータ、電子すかし等の機能を用いることで、コンテンツの権利保護を行い、特に権利情報等が格納されているメタデータとコンテンツを送信側で暗号化し、受信側で再暗号化等の処理を行いＨＤＤに暗号がかかった状態で蓄積することでコンテンツの権利保護を行うことができる。また、本発明によると、視聴契約後にコンテンツとメタデータの暗号化の鍵を個人用可搬ＣＡモジュールに格納することにより、他ＰＤＲでコンテンツを視聴する際にも権利保護が可能となる。
【図面の簡単な説明】
【図１】本発明に関する総合データ配信サービスの全体構成図。
【図２】リアルタイム視聴とサーバー型視聴の比較。
【図３】送信側において暗号化されたコンテンツ、メタデータの暗号形態の説明図。
【図４】BS伝送路暗号の暗号化データ及び鍵の伝送方法。
【図５】コンテンツ鍵Kkをメタデータを用いて伝送する場合のコンテンツ、メタデータの伝送方法。
【図６】送信側の暗号化手順を示すフローチャート。
【図７】送信側の配信手順を示すフローチャート。
【図８】受信側手順を示すフローチャート。
【図９】受信端末の基本構成図。
【図１０】ＰＤＲ内における機能ブロック図。
【図１１】ＲＭＰ内における暗号処理の構成図。
【図１２】ＲＭＰ内の機能構成図。
【図１３】受信端末における、コンテンツ受信から視聴までの基本処理フローチャート。
【図１４】受信処理の処理手順と、配信時における暗号方式と蓄積時における暗号形態の関係の説明図。
【図１５】伝送路暗号の復号処理手順を示す図。
【図１６】蓄積処理手順(1/2)を示す図。
【図１７】蓄積処理手順（2/2）を示す図。
【図１８】検索処理手順（1/2）を示す図。
【図１９】検索処理手順（2/2）を示す図。
【図２０】視聴契約処理手順を示す図。
【図２１】課金処理手順を示す図。
【図２２】メタデータ処理手順を示す図。
【図２３】コンテンツ復号手順（1/2）を示す図である。
【図２４】コンテンツ復号手順（2/2）を示す図である。
【図２５】契約コンテンツの移動ありで契約者視聴の場合の説明図。
【図２６】契約コンテンツの移動なしで契約者視聴の場合の説明図。
【図２７】公衆環境における視聴契約の処理フロー。
【図２８】通常サービスとギフトサービスの相違点を示す図。
【図２９】リムーバブルメディアに格納される情報の概要図。
【図３０】リムーバブルメディアに格納される情報。
【図３１】保護方法と目的、機能の説明図。
【図３２】本発明に関する総合データ配信サービスの全

体構成図。
【図３３】受信端末が嗜好性を判断するための必要な情報の説明図。
【図３４】ＣＡＳ用カード、ＲＭＰ用カードの特徴の説明図。
【図３５】ＰＤＲに常時固定させる必要がある情報の説明図。
【図３６】ＰＤＲより可搬させることが可能な情報の説明図。
【図３７】全体プロファイルの主な項目、内容の説明図。
【図３８】鍵テーブルと検索テーブルの内容についての説明図。
【図３９】ＲＭＰの各機能とその際に用いられる情報エリアの関係図。
【図４０】内蔵ＨＤＤ蓄積における基本処理手順との相違点の説明図。
【図４１】通常契約とギフト契約の、処理対象の相違点の説明図。
【図４２】ギフト鍵（固有鍵）の種類の説明図。
【図４３】メタデータを用いたコンテンツ鍵伝送方式における処理手順の説明図。
【図４４】コンテンツ鍵伝送方式における処理手順のフローチャート。
【図４５】リムーバブルメディアへのコンテンツ蓄積処理手順のフローチャート。
【図４６】コンテンツ視聴処理手順のフローチャート。
【図４７】メタデータを用いた蓄積後視聴のデータの流れについての説明図。
【図４８】リムーバブルメディアに蓄積後視聴のデータの流れについての説明図。
【符号の説明】
１００・・・受信部、１０１・・・限定受信暗号デスクランブラ、１０２・・・ＨＤＤ、１０３・・・著作権保護暗号デスクランブラ、１０４・・・デコーダ、１１０・・・コンテンツ鍵Kk、１１１・・・メタデータにKkを埋め込み、１１２・・・Kw2、１１３・・・スクランブル鍵Ks、１２０・・・コンテンツをKkで暗号化、１２１・・・Kkをメタデータに格納、１２２・・・メタデータをKw2で暗号化、１２３・・・コンテンツ、メタデータをエンコード、１２４・・・TSPをKsで暗号化、１２５・・・Kw2をKmcで暗号化しEMMで配信、１２６・・・Kw1をKm1で暗号化しEMMで配信、１２７・・・イベントを配信、１２８・・・KsをKw1で暗号化しECMで配信、１２９・・・Kw1入手、１３０・・・Ks入手、１３１・・・イベント入手、１３２・・・Kw2入手、１３３・・・メタデータをKw2で復号、１３４・・・メタデータよりKk入手、１３５・・・メタデータをKkで暗号化、１３６・・・コンテンツ、メタデータをＨＤＤ蓄積、１３７・・・メタデータをＨＤＤから読み出し、１３８・・・メタデータをKkで復号、１３９・・・メタデータの一部をＲＭＰ用カードに蓄積、１４０・・・Kkでコンテンツ復号、２００・・・ＲＭＰ、２０１・・・ＣＡＳ用カード、２０２・・・ＲＭＰ用カード、２１０・・・受信処理、２１１・・・ＣＡＳ、２１２・・・ＲＭＰ、２１３・・・アクセス可能ＨＤＤ、２１４・・・アクセス不可ＨＤＤ、２１５・・・ＲＭＰ、２５０・・・限定受信暗号デスクランブル、２５１・・・ＨＤＤ、２５２・・・著作権保護暗号デスクランブラ、３００・・・メタデータをKw2で復号、３０１・・・メタデータの情報を検索テーブルに格納、３０２・・・メタデータからKk入手、３０３・・・メタデータをKkで暗号化、３１０・・・コンテンツ情報表示、３１１・・・メタデータの読み込み、３２０・・・契約条件表示、３２１・・・ユーザー制限判断、３２２・・・ユーザーリクエスト判断、３３０・・・課金処理、３３１・・・視聴契約情報作成、３４０・・・視聴契約情報をメタデータに格納、３４１・・・ＲＭＰ用カードに格納、３４２・・・必要ならメタデータをKm2で暗号化、３５０・・・Kkでメタデータ復号、３５１・・・ユーザー制限の判断、３５２・・・Kkでコンテンツ復号。

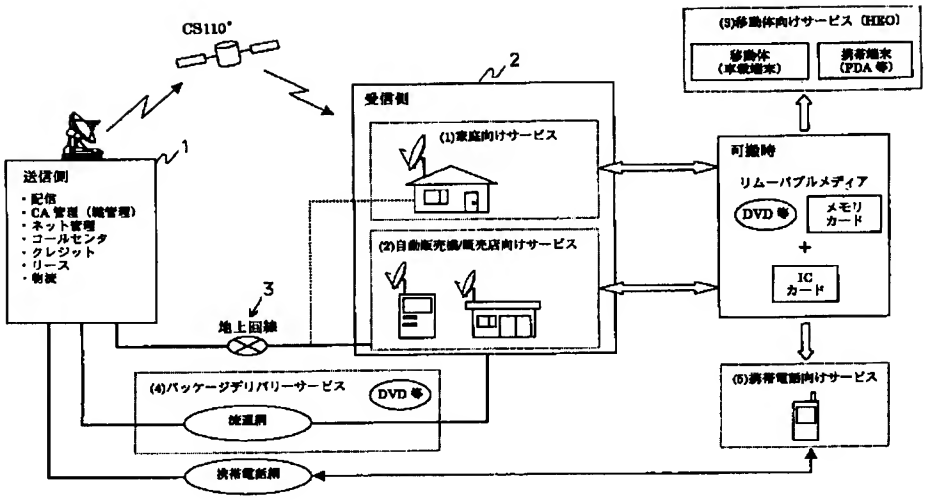
【図４】



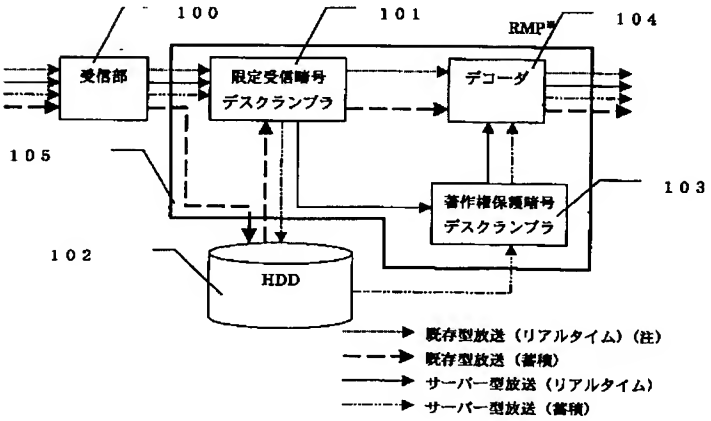
【図７】



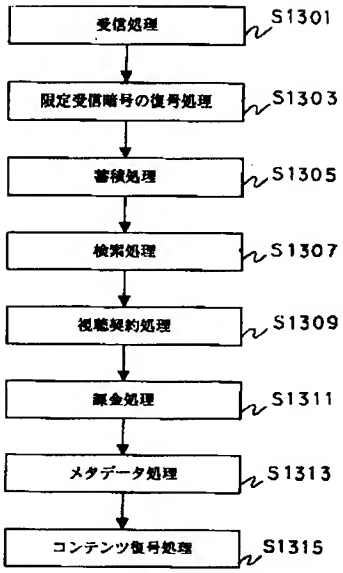
【図１】


CS110°
1
送信側
・配信
・CA管理（鍵管理）
・ネット管理
・コールセンタ
・クレジット
・リース
・物流
2
受信側
(1)家庭向けサービス
(2)自動販売機/販売店向けサービス
3
地上回線
(3)移動体向けサービス（HEO）
移動体（車載端末）
携帯端末（PDA等）
可搬時
リムーバブルメディア
DVD等
メモリカード
ICカード
(4)パッケージデリバリーサービス
DVD等
放送網
携帯電話網
(5)携帯電話向けサービス

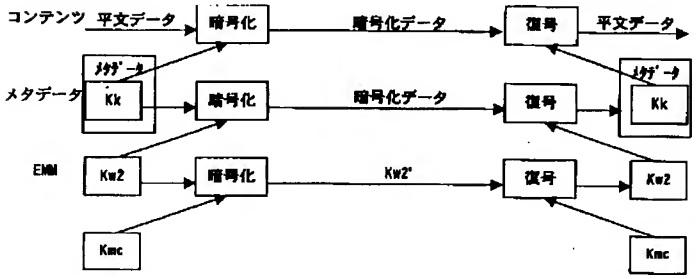
【図２】


100
101
RMP
104
受信部
限定受信暗号
デスクランブラ
デコーダ
105
103
著作権保護暗号
デスクランブラ
102
HDD
既存型放送（リアルタイム）（注）
既存型放送（蓄積）
サーバー型放送（リアルタイム）
サーバー型放送（蓄積）

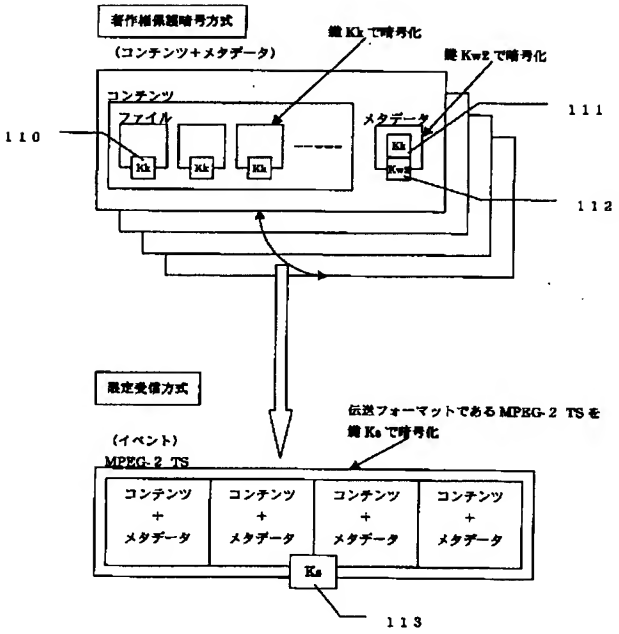
【図１３】


受信処理
S1301
限定受信暗号の復号処理
S1303
蓄積処理
S1305
検索処理
S1307
視聴契約処理
S1309
課金処理
S1311
メタデータ処理
S1313
コンテンツ復号処理
S1315

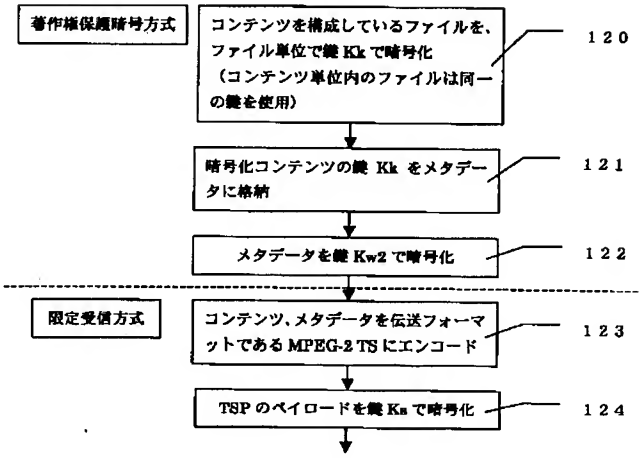
【図５】


コンテンツ
平文データ
暗号化
暗号化データ
復号
平文データ
メタデータ
Kk
暗号化
暗号化データ
復号
Kk
EMM
Kw2
暗号化
Kw2'
復号
Kw2
Kmc
Kmc

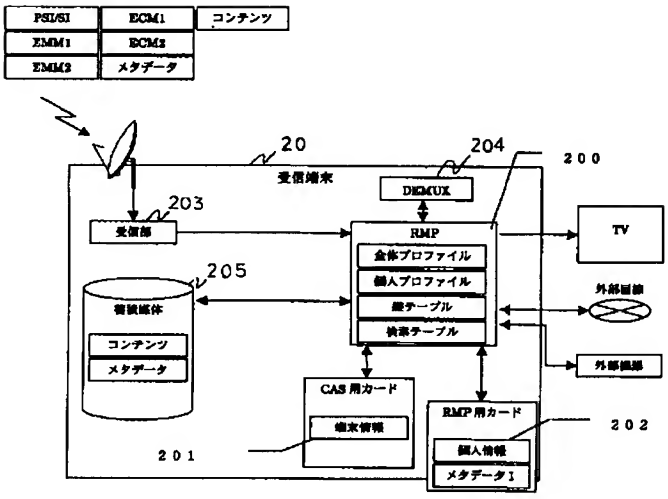
【図３】


著作権保護暗号方式
(コンテンツ+メタデータ)
鍵 Kk で暗号化
鍵 Kw2 で暗号化
コンテンツ
ファイル
メタデータ
110
111
112
限定受信方式
(イベント)
MPEG-2 TS
伝送フォーマットである MPEG-2 TS を
鍵 Ks で暗号化
コンテンツ + メタデータ
コンテンツ + メタデータ
コンテンツ + メタデータ
コンテンツ + メタデータ
113

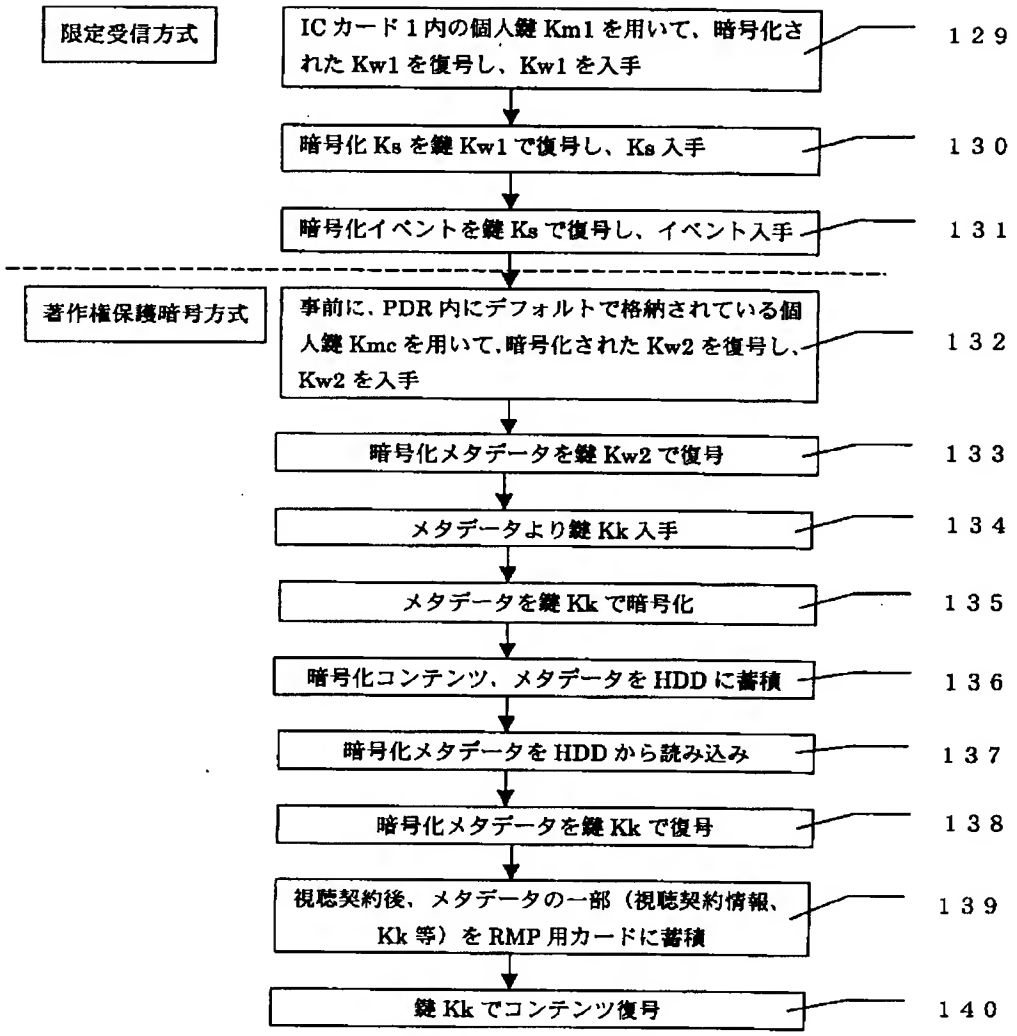
【図６】


著作権保護暗号方式
コンテンツを構成しているファイルを、ファイル単位で鍵 Kk で暗号化
（コンテンツ単位内のファイルは同一の鍵を使用）
120
暗号化コンテンツの鍵 Kk をメタデータに格納
121
メタデータを鍵 Kw2 で暗号化
122
限定受信方式
コンテンツ、メタデータを伝送フォーマットである MPEG-2 TS にエンコード
123
TSP のペイロードを鍵 Ks で暗号化
124

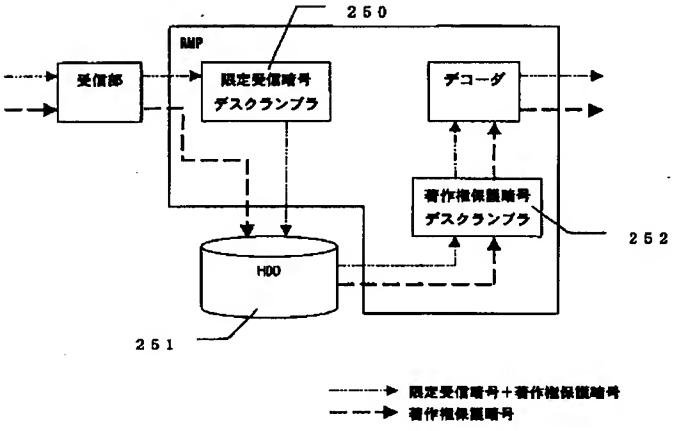
【図９】


PSI/SI
ECM1
コンテンツ
EMM1
ECM2
EMM2
メタデータ
20
受信端末
204
200
DEMUX
203
受信部
RMP
TV
205
個人プロファイル
鍵テーブル
検索テーブル
外部回線
記録媒体
コンテンツ
メタデータ
外部機器
CAS 用カード
端末情報
RMP 用カード
202
個人情報
メタデータ 1
201

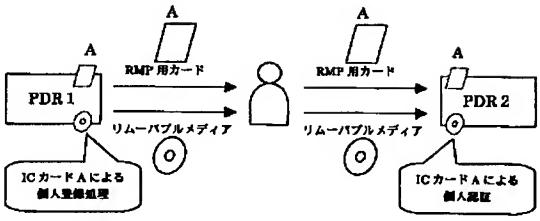
【図８】


限定受信方式
ICカード1内の個人鍵 Km1 を用いて、暗号化された Kw1 を復号し、Kw1 を入手
１２９
暗号化 Ks を鍵 Kw1 で復号し、Ks 入手
１３０
暗号化イベントを鍵 Ks で復号し、イベント入手
１３１
著作権保護暗号方式
事前に、PDR 内にデフォルトで格納されている個人鍵 Kmc を用いて、暗号化された Kw2 を復号し、Kw2 を入手
１３２
暗号化メタデータを鍵 Kw2 で復号
１３３
メタデータより鍵 Kk 入手
１３４
メタデータを鍵 Kk で暗号化
１３５
暗号化コンテンツ、メタデータを HDD に蓄積
１３６
暗号化メタデータを HDD から読み込み
１３７
暗号化メタデータを鍵 Kk で復号
１３８
視聴契約後、メタデータの一部（視聴契約情報、Kk 等）を RMP 用カードに蓄積
１３９
鍵 Kk でコンテンツ復号
１４０

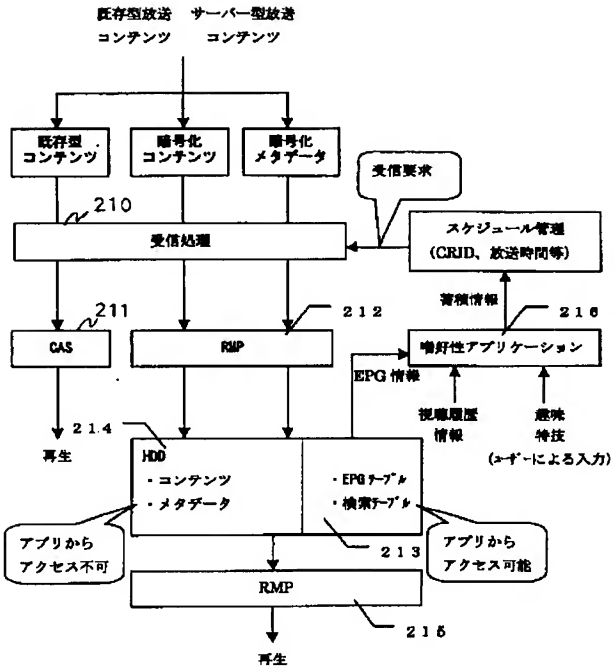
【図１１】


250
RMP
受信部
限定受信暗号デスクランブラ
デコーダ
著作権保護暗号デスクランブラ
252
HDD
251
限定受信暗号＋著作権保護暗号
著作権保護暗号

【図２５】


A
PDR 1
RMP 用カード
リムーバブルメディア
ICカードAによる個人登録処理
A
RMP 用カード
リムーバブルメディア
A
PDR 2
ICカードAによる個人認証

【図１０】

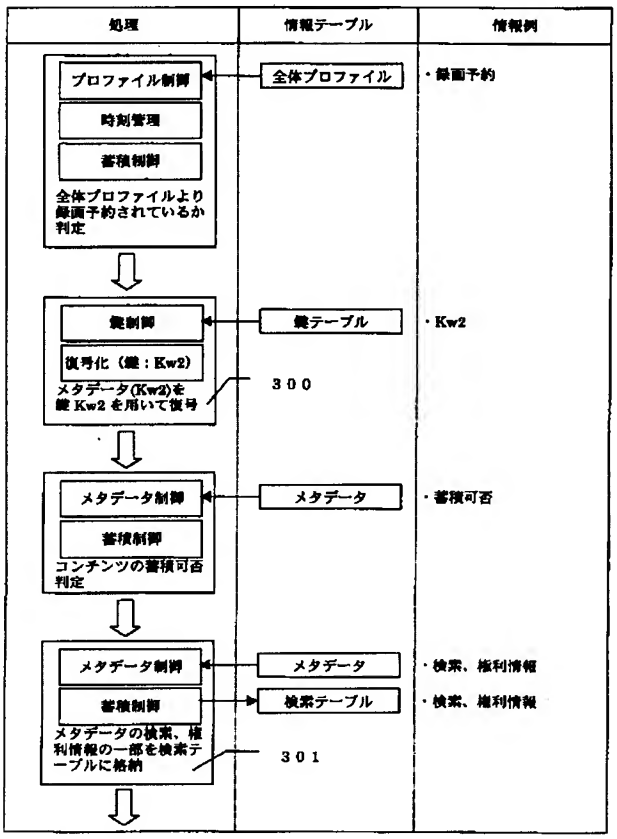


【図１４】

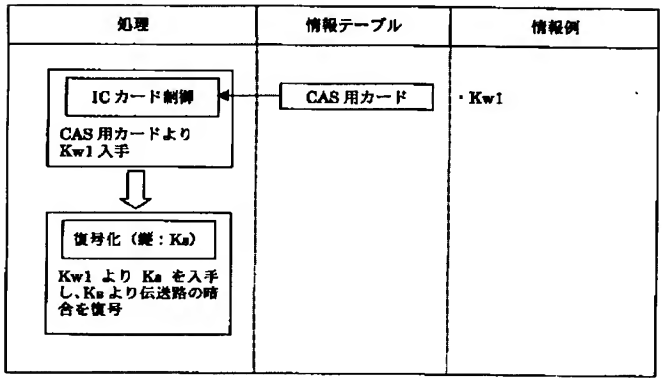
処理	情報テーブル	情報例
受信制御 復号処理を選択	PSI/SI	

	CASE①	CASE②	CASE③	CASE④
固定受信方式蓄積	×	○	×	×
著作権保護暗号方式蓄積	○	×	○	×
暗号なし蓄積	○	○	○	○

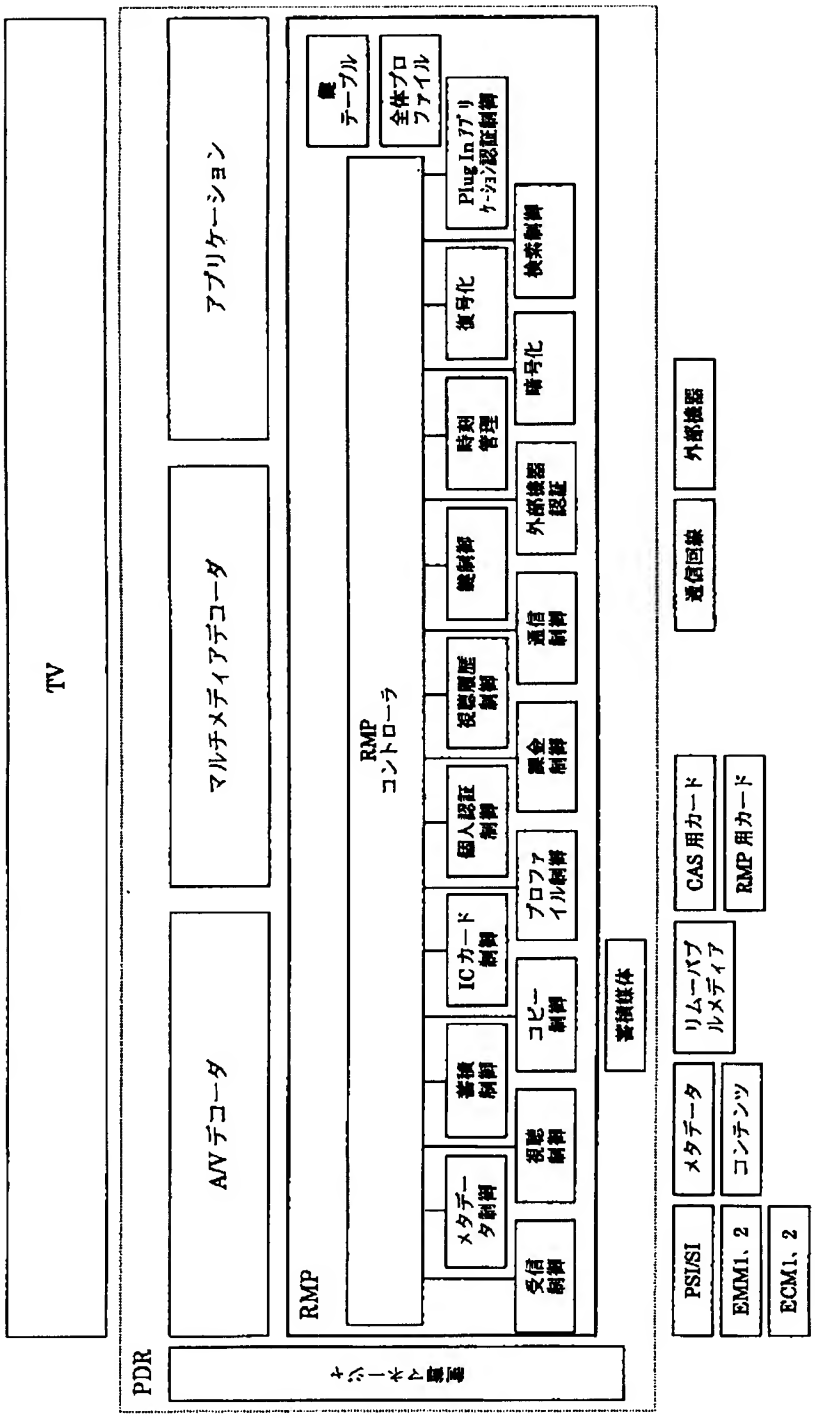
【図１６】



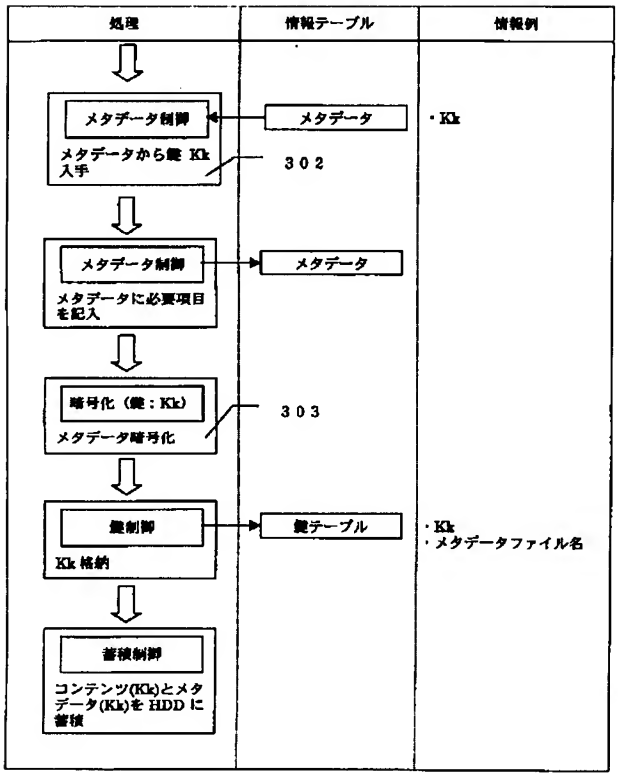
【図１５】



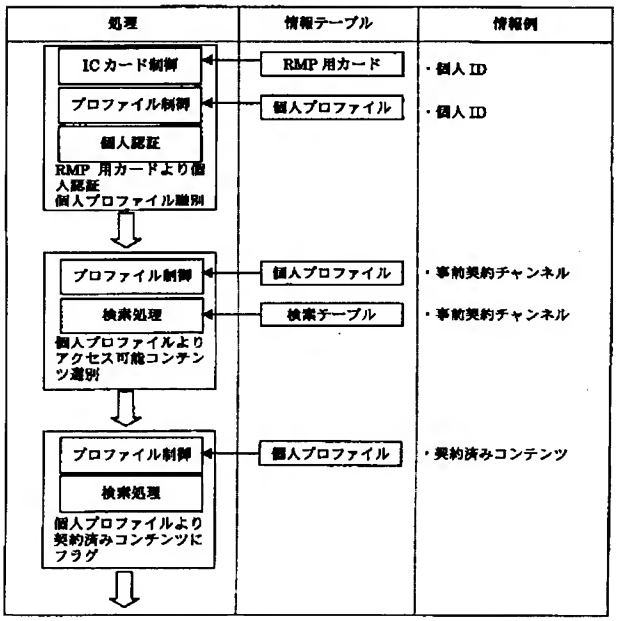
【図１２】


TV
PDR
ネットワーク層
A/Vデコーダ
マルチメディアデコーダ
アプリケーション
RMP
RMP
コントローラ
鍵テーブル
全体プロファイル
Plug In アプリケーション認証制御
メタデータ制御
蓄積制御
ICカード制御
個人認証制御
視聴履歴制御
課金制御
通信制御
外部機器認証
時刻管理
暗号化
検索制御
受信制御
視聴制御
コピー制御
プロファイル制御
機制御
復号化
蓄積媒体
PSI/SI
メタデータ
リムーバブルメディア
CAS用カード
通信回線
外部機器
EMM1、2
コンテンツ
RMP用カード
ECM1、2

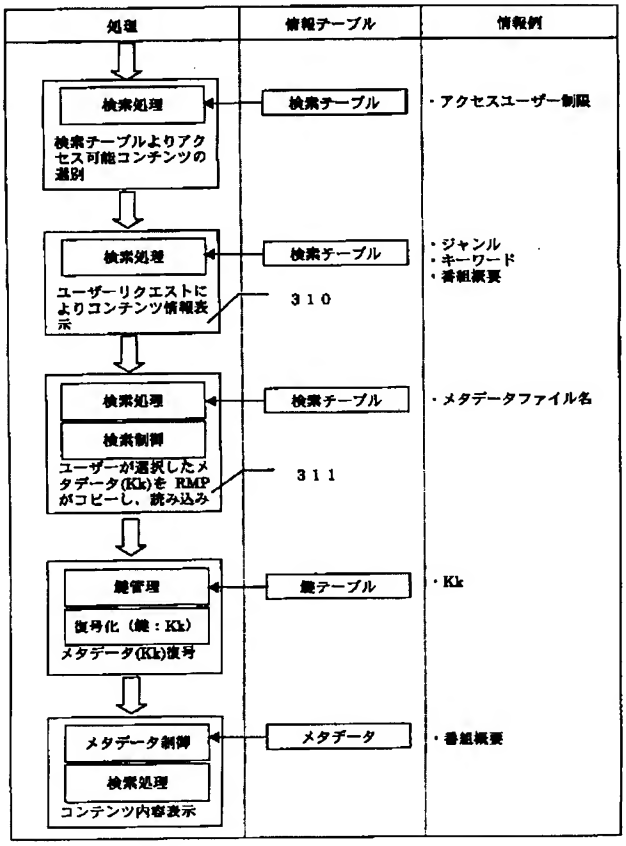
【図１７】



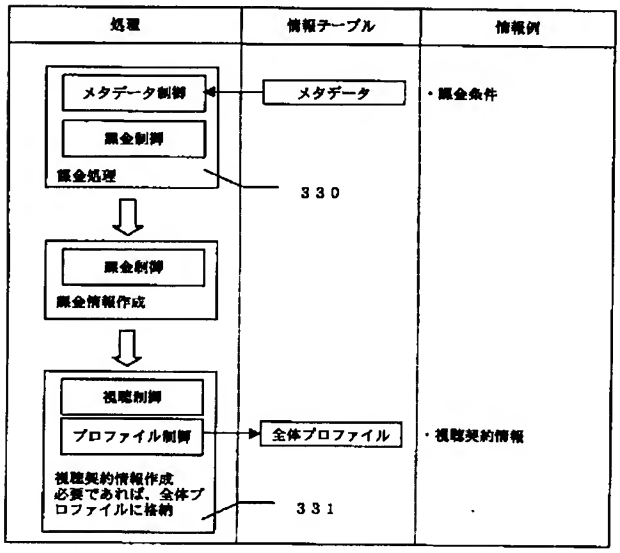
【図１８】



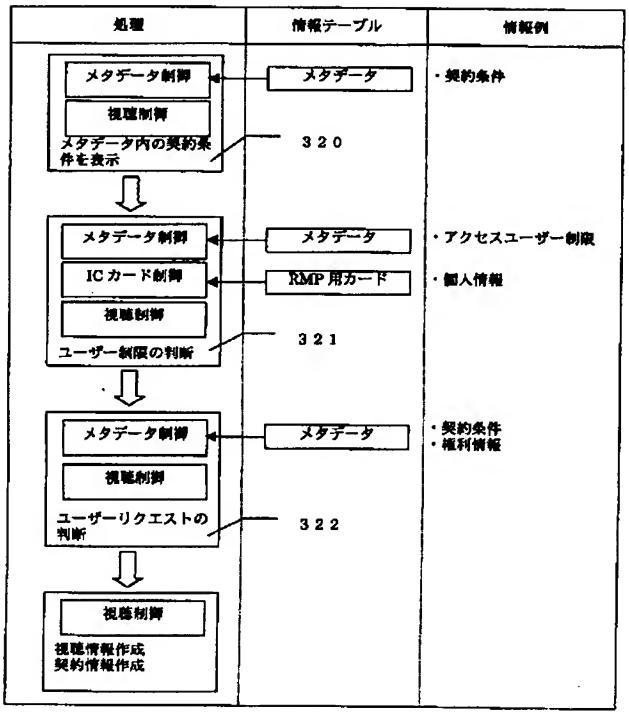
【図１９】



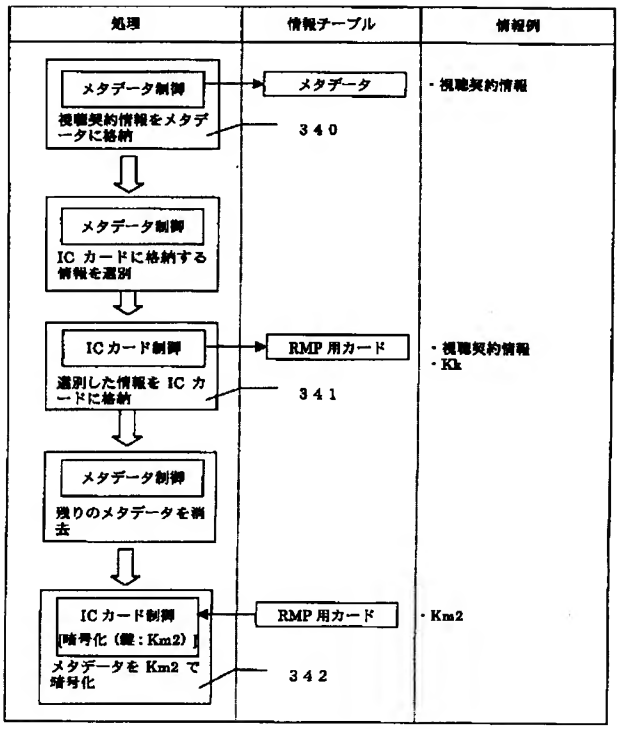
【図２１】



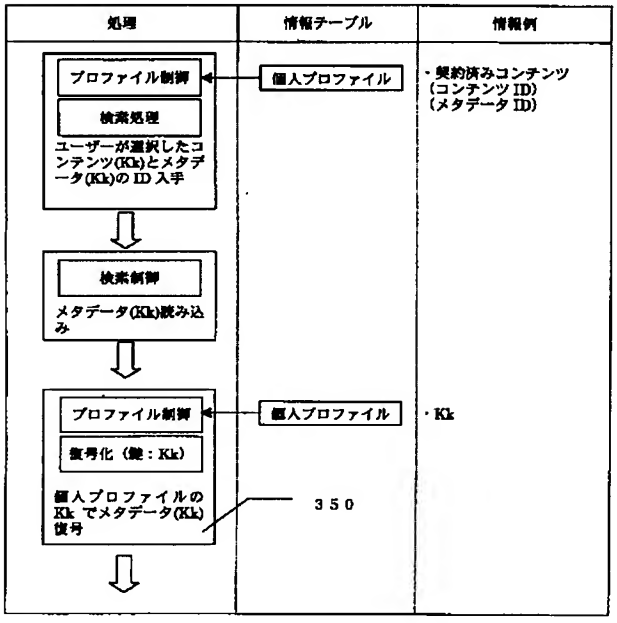
【図２０】



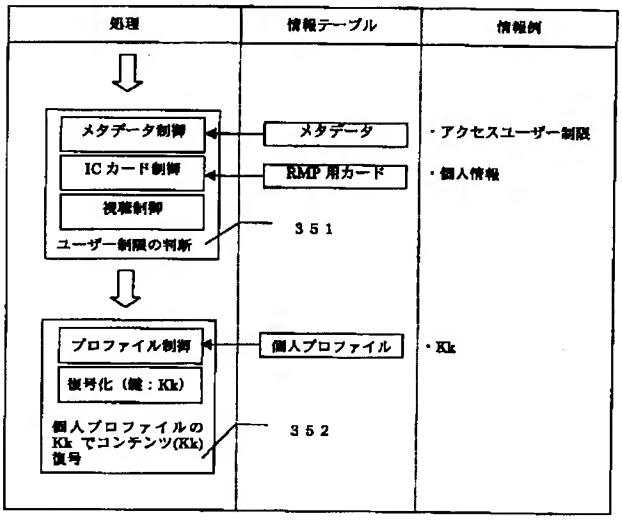
【図２２】



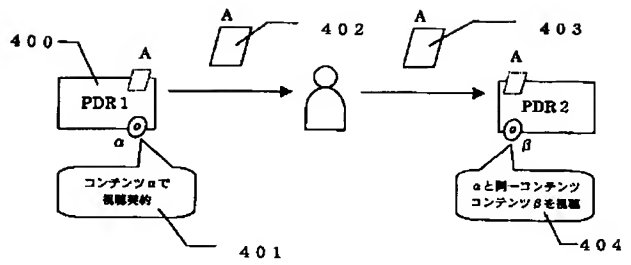
【図２３】



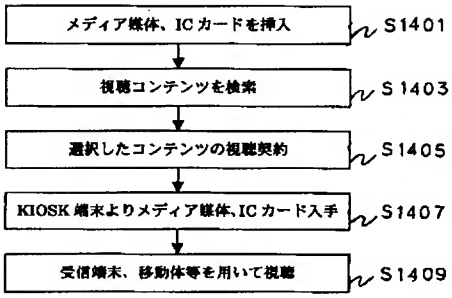
【図２４】



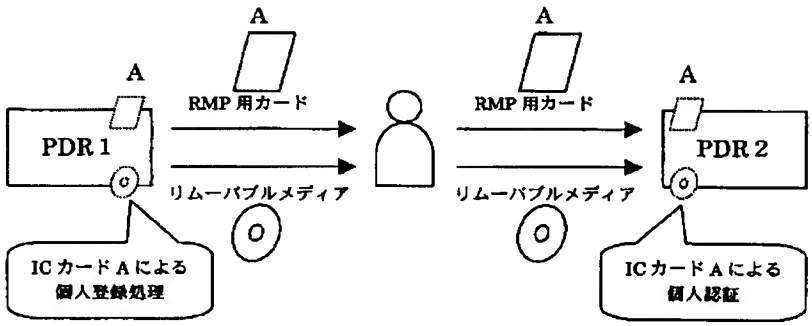
【図２６】

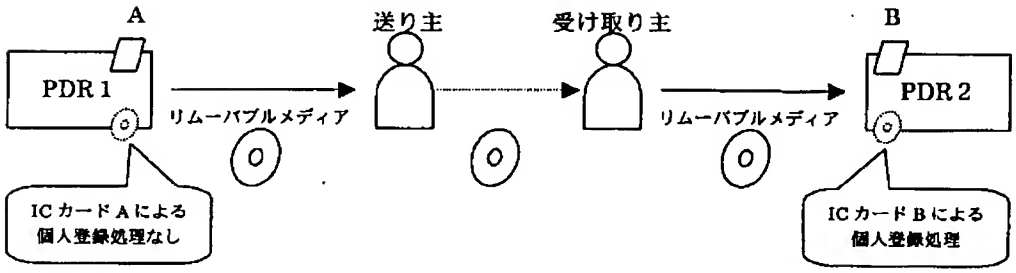

400
A
PDR 1
α
コンテンツαで視聴契約
401
A
402
A
403
A
PDR 2
β
αと同一コンテンツコンテンツβを視聴
404

【図２７】

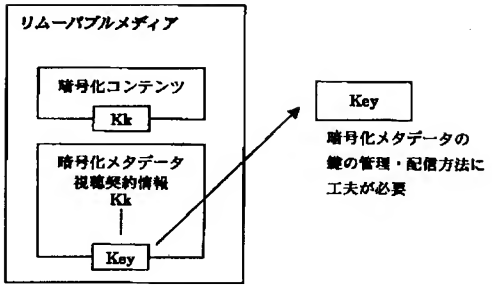

メディア媒体、ICカードを挿入
S1401
視聴コンテンツを検索
S1403
選択したコンテンツの視聴契約
S1405
KIOSK端末よりメディア媒体、ICカード入手
S1407
受信端末、移動体等を用いて視聴
S1409

【図２８】

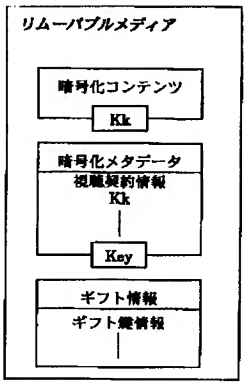

A
A
RMP用カード
PDR 1
リムーバブルメディア
ICカードAによる個人登録処理
A
A
RMP用カード
PDR 2
リムーバブルメディア
ICカードAによる個人認証


A
PDR 1
リムーバブルメディア
ICカードAによる個人登録処理なし
送り主
受け取り主
B
リムーバブルメディア
PDR 2
ICカードBによる個人登録処理

【図２９】



【図３０】



【図３１】

保護方法	目的例	機能
暗号化	情報の不正な書き換え防止	コンテンツ、メタデータの暗号化
	情報の不正な視聴防止	コンテンツ、メタデータの暗号化
個人認証	サービスプロバイダ、著作権所有者の、コンテンツへのユーザーアクセス制限権利の保護	著作権情報、権利情報のユーザーアクセス制限と個人情報との照らし合わせ
	ユーザーのコンテンツ視聴権利の保護	個人単位の契約情報に沿ったコンテンツにアクセス
	プライバシーの保護	個人情報へのアクセス
メタデータ	著作権情報、権利情報の使用	コンテンツとセットで用い、そのコンテンツの著作権情報、権利情報を格納
電子すかし	コンテンツに対する不正使用の抑止	コンテンツの不正使用時にアプリケーションより使用不可が可能。

【図３２】

構成	
送出側	・送信センタ ・鍵管理センタ ・地上回線管理センタ ・顧客管理センタ ・物流管理センタ
受信側	・受信端末 ・KIOSK 端末 ・販売店 ・（T-Station） ・（移動体） ・（携帯電話）
伝送路	・衛星 ・地上回線 ・流通網 ・（携帯電話網）

() 内は拡張

【図３３】

処理形態	情報入手先	情報例
受信端末の能動的処理	ユーザーが受信端末に対して情報を入力（ユーザーの意思あり）	・ジャンル ・キーワード ・職業 ・趣味　　等
受信端末の自律的処理	受信端末がユーザー情報から情報を入手（ユーザーの意思なし）	・視聴履歴 ・検索履歴 ・個人情報　等

【図３４】

	CAS用カード	RMP用カード
配布単位	受信端末に１枚	個人に１枚
可搬性	なし（受信端末内に常時装備）	あり（個人が携帯）
視聴権利単位	家族、グループ	個人、(グループ※)
課金単位	家族、グループ	個人、(グループ※)
関連暗号	限定受信方式	K暗号方式
課金対象物	サービス、イベント	コンテンツ
視聴契約方法	事前契約方法	事前契約方式＋視聴時契約方式

※　グループ契約の時

【図３５】

項目	内容
ＰＤＲ使用者情報	個人用可搬ＣＡモジュールの纏めた情報（例カードＩＤ等）
蓄積装置内の暗号情報	・コンテンツの暗号情報 ・メタデータの暗号情報
蓄積装置内の検索情報	コンテンツのメタデータ情報
蓄積装置内のリソース管理情報	コンテンツの有効期限、視聴制限等に関する情報

(A)

項目	内容
カードID	・EMMを取得する際に、自分自身宛の情報かを識別するために必要となる情報。
有料事業体識別	・端末利用ユーザーが契約する事業体のコードであり、これにより限定受信コンテンツが契約コンテンツであるかを識別する
契約情報 ・ワーク鍵Kw識別 ・ワーク鍵Kw	有料放送契約に関する情報。 ・ECMのワーク鍵Kw識別により照合するための情報 ・ECMの暗号を復号するために必要となる情報
定期発呼日時	・センタ側から視聴履歴、課金履歴等の発呼日時を指定するために必要となる情報

(B)

【図３７】

項目	内容
グループID	・EMM2を取得する際に自身宛ての情報かを判定することに利用
利用ユーザーID（個人ID）	・EMM2、ECM2等で得られる情報を受信端末を利用するユーザーに割り振ることに利用
グループ員ID	・グループ契約の際のグループ員全員のID
事業体コード	・コンテンツを蓄積する際に契約コンテンツかを判定することに利用
事前契約事業体コード	・全受信端末使用者の事前契約（ティア）事業体コード
契約識別	・登録された事業体コードがどのユーザーによるものかを判定することに利用
スケジュールに関する情報	・録画予約の重複を監視、予約実行の指示出しに利用
ユーザー嗜好性	・全てのユーザーの嗜好性 ・HDDにコンテンツを選定して蓄積する際に利用
個人ID	・受信端末に挿入されたICカード2に対応するプロファイルを識別する際に利用
個人情報	・利用者名、グループの属性、年齢、性別、住所、電話番号、クレジット番号、口座番号等の情報
パスワード	・各種認証が必要な際に利用する
事前契約事業体コード	・事前契約を行った事業体コード
契約済みコンテンツ	・本人もしくはグループ員がグループ契約で視聴契約を行ったコンテンツ
視聴情報	・視聴、蓄積を行なった番組名、ジャンル等が格納されており視聴履歴、ユーザーの嗜好性を抽出する際に利用
契約情報	・有効期限、有効回数、視聴条件等の契約情報が格納されており、視聴時に契約条件を満たしているか判定する際に利用
課金情報	・課金方法、指定口座情報、課金済みフラグ等の課金に関する情報が格納されており課金処理時に利用する。

【図４１】

処理	処理対象			
	通常契約		ギフト契約	
	受信端末	RMP用カード	受信端末	RMP用カード
視聴契約処理	1	A	1	A
課金処理	1	A	1	A
所有者登録処理	1	A	2	B
視聴	2	A	2	B

（注）表中の数字、アルファベットは図２５参照

【図３６】

項目	内容
個人 ID	・個人認証などに必要となるＩＤ
個人情報	・利用者名、グループの属性、年齢、性別、住所、電話番号、クレジット番号、口座番号等の情報
事前契約事業体コード	・事前契約を行った事業体コード
メタデータ	・本人が視聴契約をおこなったコンテンツのメタデータ
メタデータ ID	・ユーザーが視聴契約を行ったコンテンツのメタデータを識別する際に必要となる情報。
コンテンツ ID	・ユーザーが視聴契約を行ったコンテンツを識別する際に必要となる情報。
視聴情報	・視聴、蓄積を行なった番組名、ジャンル等が格納されており視聴履歴、ユーザーの嗜好性を抽出する際に利用
契約情報	・有効期限、有効回数、視聴条件等の契約情報が格納されており、視聴時に契約条件を満たしているか判定する際に利用
課金情報	・課金方法、指定口座情報、課金済みフラグ等の課金に関する情報が格納されており課金処理時に利用する。
契約状態	・課金済みか等を識別する際に必要となる情報

【図３８】

項目		内容
鍵 Kw2 関連情報	事業体コード	・プロファイルから鍵を識別する際に使用
	ワーク鍵 Kw2	・鍵自身を格納
鍵 Kk 関連情報	メタデータ ID (コンテンツ ID)	・どのメタデータに対する暗号鍵かを識別するために利用
	鍵 Kk	・鍵自身を格納
鍵 Kmc 関連情報	鍵 Kmc	・鍵自身を格納

(A)

項目	内容
コンテンツ ID	・各処理において、目的のコンテンツを識別するための情報
コンテンツ名	・ユーザーに提示するための情報
コンテンツ蓄積場所	・目的のコンテンツを引っ張る際に必要となる情報
メタデータ ID	・各処理において、目的のコンテンツを識別するための情報
メタデータ蓄積場所	・コンテンツに対応するメタデータを引っ張る際に必要となる情報
ジャンル	・検索アプリケーション内のサービスとして必要な情報
キーワード	・検索アプリケーション内のサービスとして必要な情報
概要	・検索アプリケーション内のサービスとして必要な情報
アクセスユーザー制限情報	・当該コンテンツを視聴可能なユーザーか、判断するための情報（年齢、性別等）
事業者コード	・各ユーザーが利用可能なコンテンツを識別する際に必要となる情報

(B)

【図４０】

項目	基本処理 (内蔵 HDD 蓄積)	受信端末外視聴 (リムーバブルメディア蓄積)
視聴契約処理	視聴契約において「視聴」選択	視聴契約において「蓄積」選択
	RMP が、「視聴条件」を満たしているか判断	RMP が、「蓄積条件」を満たしているか判断
メタデータ処理	メタデータ２を「HDD」に蓄積	メタデータ２を「リムーバブルメディア」に蓄積
リムーバブルメディア蓄積	—	「暗号化コンテンツをリムーバブルメディアに蓄積」
コンテンツ復号	「個人プロファイル」の情報を用いて、契約済みコンテンツを「HDD」から読み込む	「IC カード２の情報をゲストプロファイルに書き込み、」「ゲストプロファイル」の情報を用いて、契約済みコンテンツを「リムーバブルメディア」から読み込む

(A)

項目	基本処理 (内蔵 HDD 蓄積)	受信端末外視聴 (コンテンツの移動なし)
メタデータ処理	メタデータをメタデータ１、メタデータ２に分離	メタデータ分離はしない
	メタデータ１を個人鍵 Km2 で暗号化し、IC カードに蓄積 メタデータ２を使い捨て鍵 Kr'で暗号化し、HDD に蓄積	メタデータを個人鍵 Km2 で暗号化し、IC カードに蓄積
コンテンツ復号	「個人プロファイル」の情報を用いて、契約済みコンテンツを「HDD」から読み込む	「IC カード２の情報をゲストプロファイルに書き込み、」「ゲストプロファイル」の情報を用いて、契約済みコンテンツを「リムーバブルメディア」から読み込む
	メタデータ１、２とコンテンツがそろってコンテンツの復号処理	メタデータとコンテンツがそろってコンテンツの復号処理

(B)

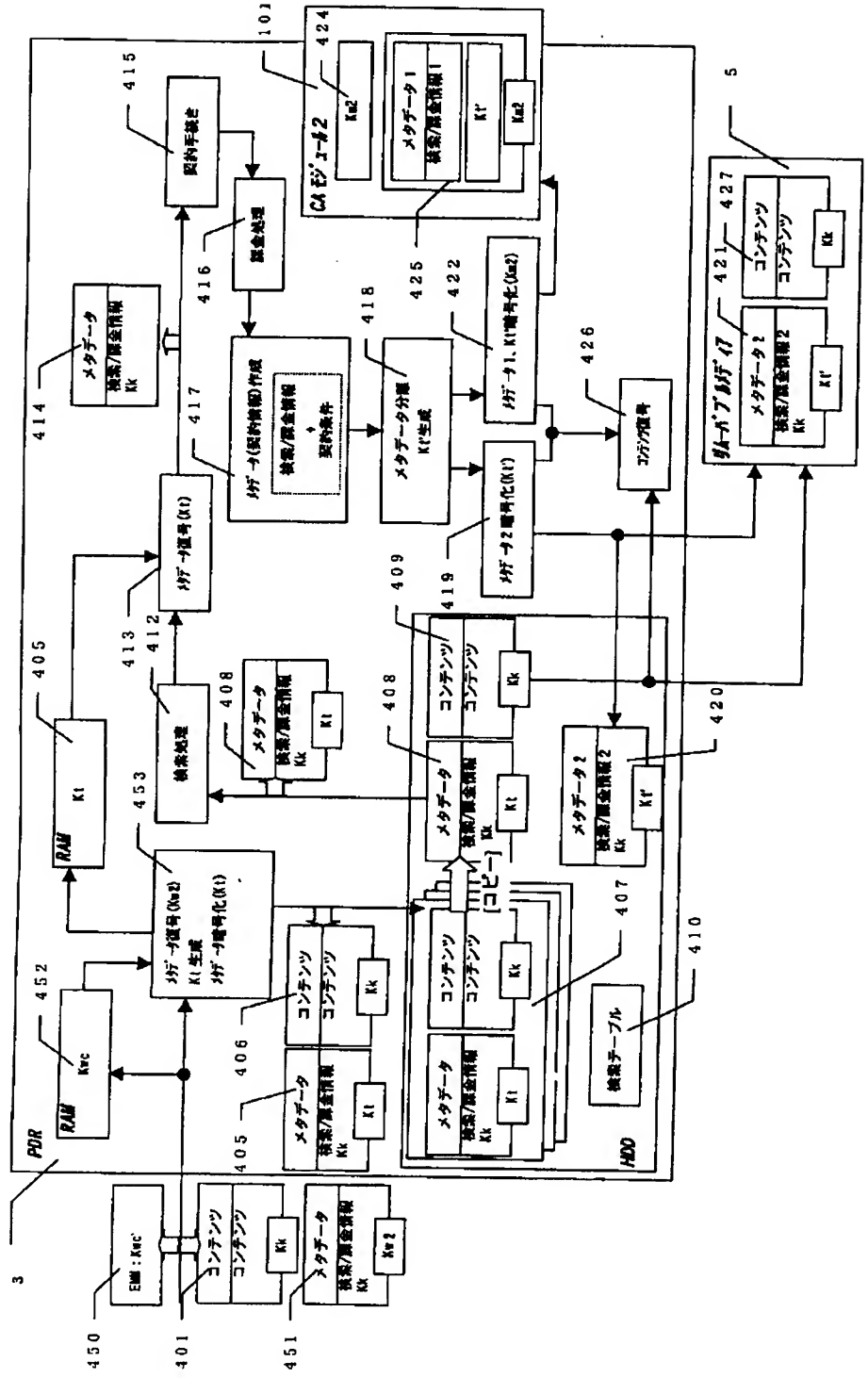
【図３９】

	機能	情報エリア						
		メタデータ	鍵テーブル	プロファイル		CAカード		PSI/SI
				全体	個人	1	2	
①	受信制御							○
②	蓄積制御	○		○				
③	コピー制御	○						
④	視聴制御	○			○		○	
⑤	課金制御	○			○			
⑥	暗号化		○					
⑦	復号化	○	○			○		
⑧	個人認証				○		○	
⑨	視聴履歴制御	○			○			
⑩	外部機器認証	○	○					
⑪	通信制御	○	○				○	
⑫	メタデータ制御	○						
⑬	プロファイル制御			○	○			
⑭	鍵制御	○	○					
⑮	ICカード制御					○	○	

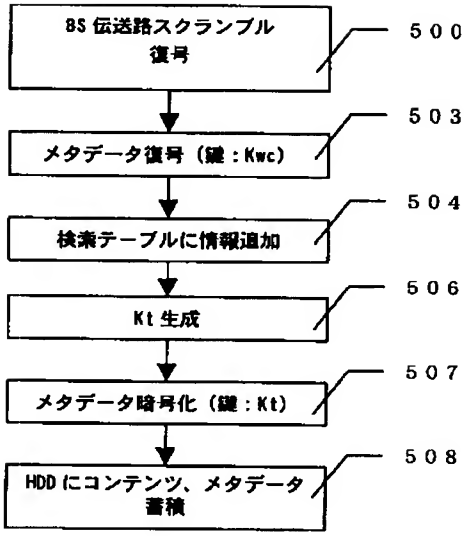
【図４２】

	ギフト鍵	特徴
①	全ての受信端末に共通の唯一な固有鍵	リムーバブルメディアにギフト鍵情報を記入しない
②	全ての受信端末に共通な，任意に用いる事が可能な数種類の固有鍵	リムーバブルメディアにギフト鍵情報を記入する
③	全ての受信端末に共通な，各サービスプロバイダ毎に指定の固有鍵	

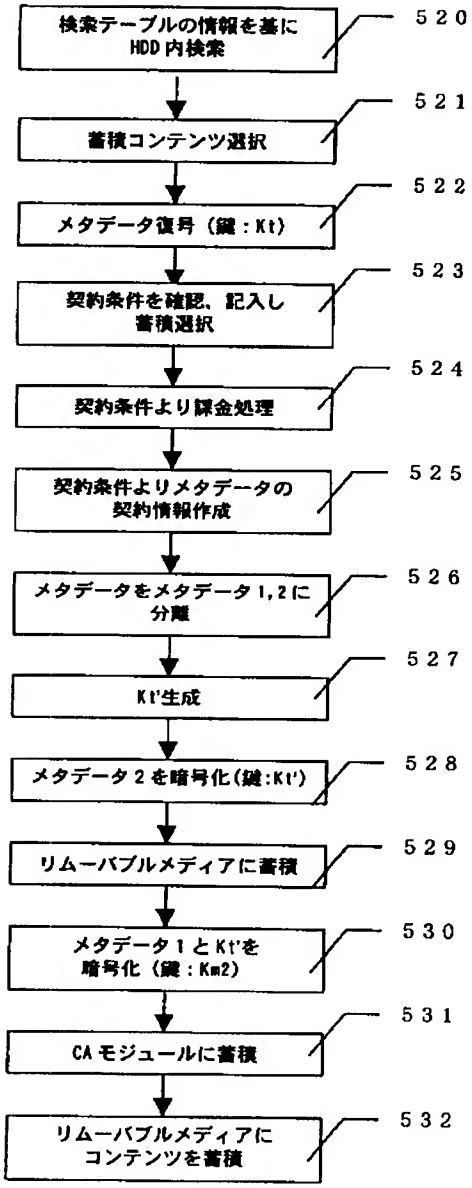
【図４３】


PDR
RAM
HDD
メタデータ
検索/課金情報
コンテンツ
検索テーブル
契約手続き
課金処理
メタデータ分離
Kt生成
エンタング暗号
[コピー]

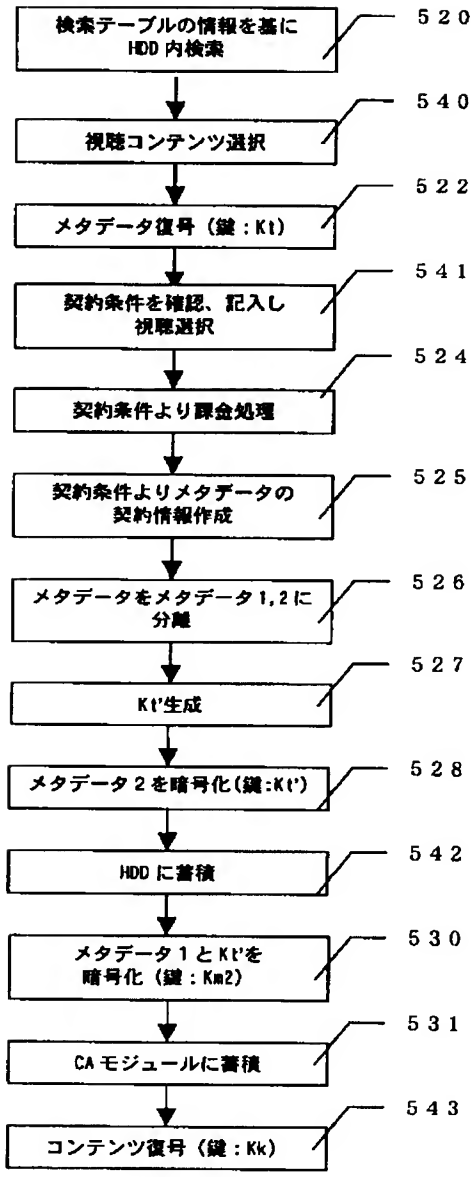
【図４４】


BS 伝送路スクランブル
復号
５００
メタデータ復号（鍵：Kwc）
５０３
検索テーブルに情報追加
５０４
Kt 生成
５０６
メタデータ暗号化（鍵：Kt）
５０７
HDD にコンテンツ、メタデータ
蓄積
５０８

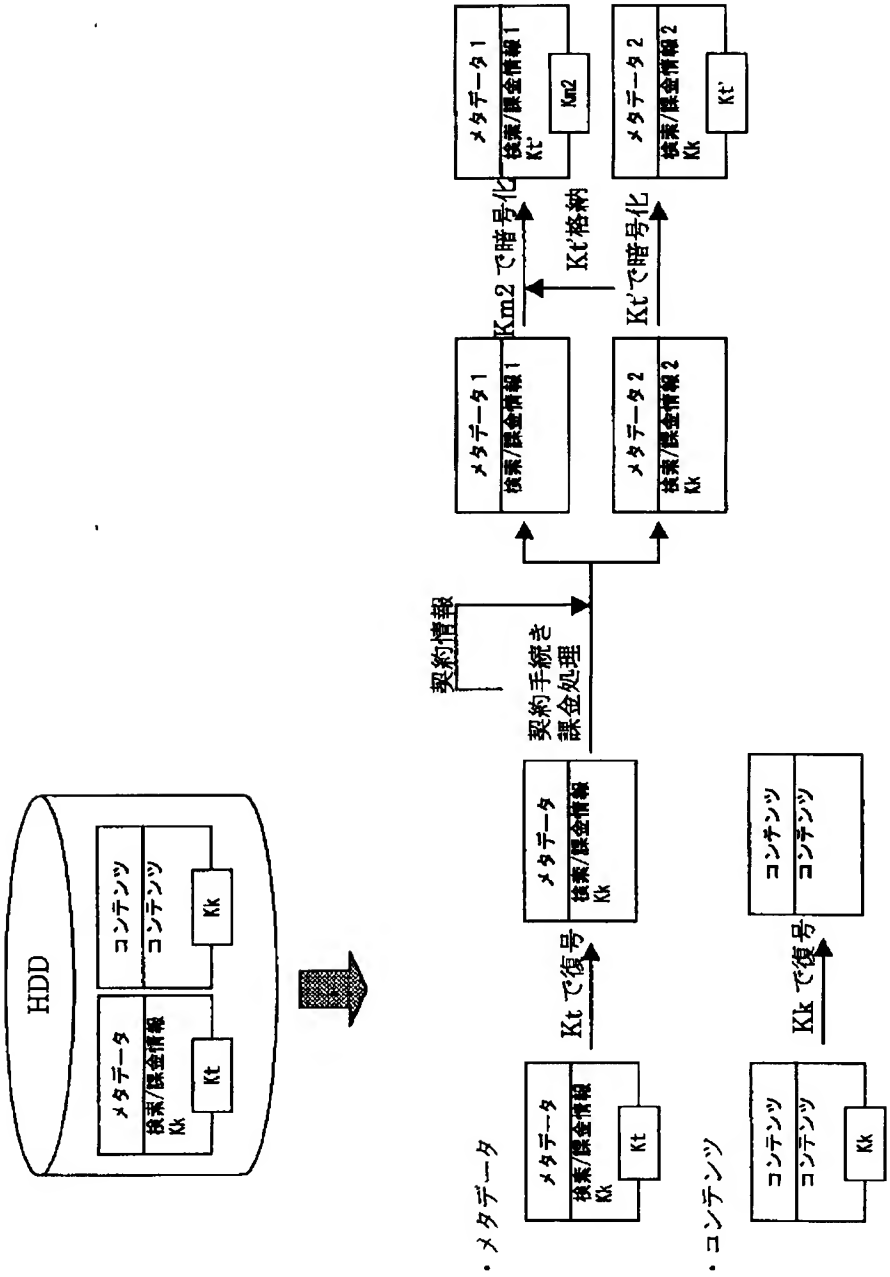
【図４５】


検索テーブルの情報を基に HDD内検索
520
蓄積コンテンツ選択
521
メタデータ復号（鍵：Kt）
522
契約条件を確認、記入し 蓄積選択
523
契約条件より課金処理
524
契約条件よりメタデータの 契約情報作成
525
メタデータをメタデータ1,2に 分離
526
Kt'生成
527
メタデータ2を暗号化(鍵:Kt')
528
リムーバブルメディアに蓄積
529
メタデータ1とKt'を 暗号化（鍵：Km2）
530
CAモジュールに蓄積
531
リムーバブルメディアに コンテンツを蓄積
532

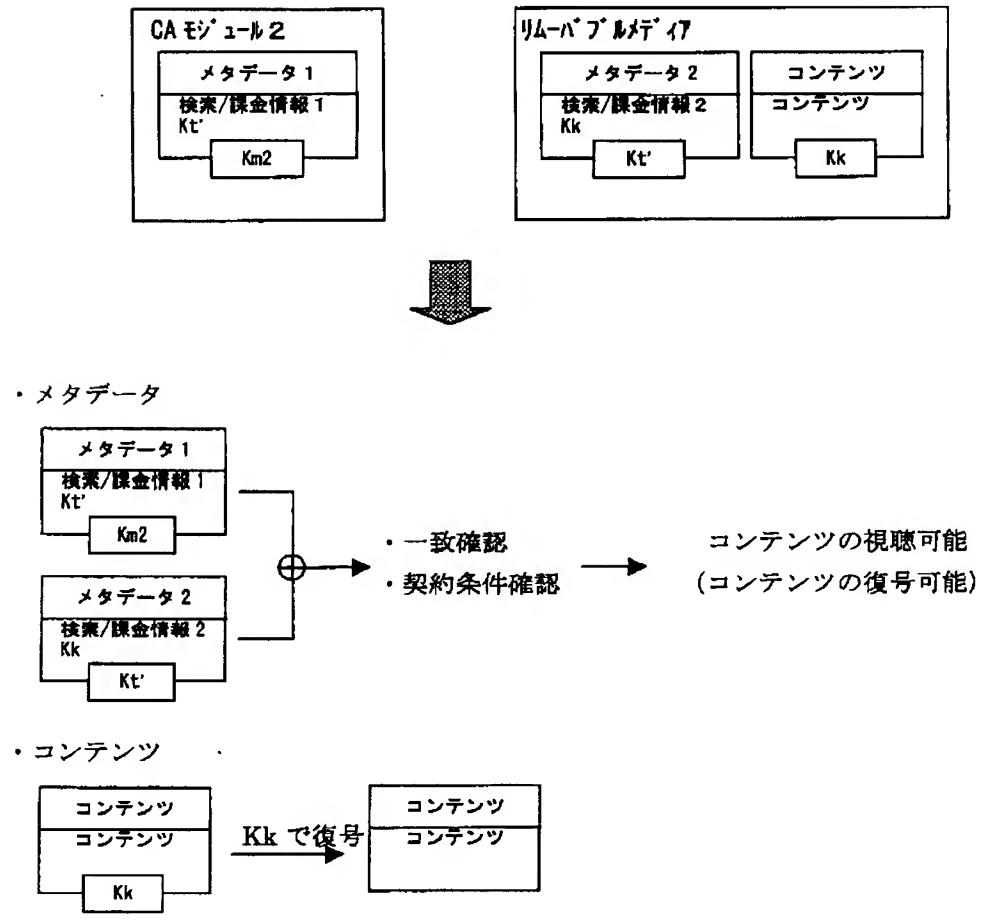
【図４６】


検索テーブルの情報を基に HDD 内検索
520
視聴コンテンツ選択
540
メタデータ復号（鍵：Kt）
522
契約条件を確認、記入し 視聴選択
541
契約条件より課金処理
524
契約条件よりメタデータの 契約情報作成
525
メタデータをメタデータ 1,2 に 分離
526
Kt'生成
527
メタデータ 2 を暗号化（鍵:Kt'）
528
HDD に蓄積
542
メタデータ 1 と Kt'を 暗号化（鍵：Km2）
530
CA モジュールに蓄積
531
コンテンツ復号（鍵：Kk）
543

【図４７】


HDD
メタデータ
検索/課金情報
Kk
Kt
コンテンツ
コンテンツ
Kk
契約情報
契約手続き
課金処理
メタデータ
検索/課金情報
Kk
Kt で復号
メタデータ
検索/課金情報
Kk
Kt
・メタデータ
コンテンツ
コンテンツ
Kk で復号
コンテンツ
コンテンツ
Kk
・コンテンツ
メタデータ 1
検索/課金情報 1
Kt'
Km2
Km2 で暗号化
Kt'格納
メタデータ 1
検索/課金情報 1
メタデータ 2
検索/課金情報 2
Kk
Kt'で暗号化
メタデータ 2
検索/課金情報 2
Kt'

【図４８】



フロントページの続き

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ	7/08	Ｚ
			7/167	Ｚ

(72)発明者　小西　薫
東京都千代田区神田駿河台四丁目６番地
株式会社日立製作所放送・通信システム推進事業部内

Ｆターム(参考)　5C053 FA13 FA23 GB01 HA40 KA04
KA05 KA21 KA24 LA06 LA15
5C063 AA01 AB03 AB07 AC01 CA23
CA29 CA36 DA07 DA13
5C064 CA14 CC02 CC04
5J104 AA01 AA12 AA16 BA03 EA01
EA04 EA17 JA03 MA06 NA03
NA35 NA37 PA05